UNIVERSITAS INDONESIA

ANALISA RISIKO KUALITATIF STUDI KASUS PADA PT ”X” PERUSAHAAN PENYEDIA JASA DATA CENTER

SKRIPSI

Diajukansebagaisyaratuntukmemperolehgelar Sarjana (S1)
Pada Program SarjanaFakultasIlmuSosialdanPpolitik

Lia de Vega

0706284396

FAKULTAS ILMU SOSIAL ILMU POLITIK

PROGRAM STUDI KRIMINOLOGI

DEPOK

JUNI,2012

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama : Lia de Vega

NPM : 0706284396

Tanda Tangan :

Tanggal :

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Lia de Vega

NPM : 0706284396

Program Studi : Kriminologi

Judul Skripsi : Analisa Risiko Kualitatif, Studi Kasus Pada PT "X" Perusahaan Penyedia Jasa Data Center

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Reguler pada Program Studi Kriminologi, Fakultas Ilmu Sosial Politik, Universitas Indonesia.

DEWAN PENGUJI

Penguji Ahli : Muhammad Nuh Al-Azhar, MSc. (.....)

Pembimbing : Drs, Dadang Sudiadi, M.Si. (.....)

Ketua Sidang : Drs. Eko Hariyanto, M.Si. (.....)

Sekertaris Sidang : Kisnu Widagso S.Sos., M.T.I. (.....)

Ditetapkan di : Depok

Tanggal : 22 Juni 2012

KATA PENGANTAR

Terima kasih penulis panjatkan kehadirat Tuhan Yang Maha Baik atas berkat dan penyertaan-Nya yang sempurna sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisa Risiko Kualitatif,Studi Kasus pada PT "X" Perusahaan Penyedia Jasa Data Center." Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk memperoleh gelar Sarjana Kriminologi. Universitas Indonesia. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu,penulis mengucapkan terima kasih kepada:

1. Drs. Dadang Sudiadi M,Si selaku dosen pembimbing yang telah smeluangkan waktu, tenaga dan pikiran serta sabar dalam membimbing dan mengarahkan penulis untuk menyelesaikan skripsi ini
2. Para dosen kriminologi yang telah membimbing penulis dalam masa perkuliahan
3. Pihak PT "X" yang tidak dapat disebutkan satu persatu, dari informan hingga teman satu tim penulis yang telah mendukung dengan memberikan data,informasi serta meluangkan waktu untuk bersedia diwawancara, tanpa kesediaan teman-teman dari PT "X" skripsi ini tidak akan berjalan dengan baik.
4. Orang tua dan kedua adik penulis yang selalu mendampingi penulis bahkan dalam saat-saat berat dalam menyelesaikan skripsi ini.
5. Teman-teman kriminologi 2007 especially for alfin deska and Benita nastami! Thanks for you guys willingness to help me and giving some advices

6. Nelson panjaitan, thank you for your willingness!
7. Semua pihak yang tidak dapat disebutkan satu persatu, terimakasih semuanya yang telah membantu,mendoakan penulis hingga dapat menyelesaikan skripsi ini

Depok,8 Juni 2012

Penulis

ALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS

AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini :

Nama	: Lia de Vega
NPM	: 0706284396
Program Studi	: Kriminologi
Departemen	: Kriminologi
Fakultas	: Ilmu Sosial Ilmu Politik
Skripsi	: Skripsi

Demi pembangunan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif** ***(Non-Exclusive Royalty Right)*** atas karya ilmiah saya yang berjudul:

Analisa Risiko Kualitatif (Studi Kasus pada PT "X" Perusahaan Penyedia Jasa Data Center

Beserta perangkat yang ada (jika diperlukan). Dengan hak bebas royalty non eksklusif ini. Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database) merawat dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta.

Demikian

Dibuat di : Depok

Pada Tanggal : 22 Juni 2012

Yang Menyatakan :

(Lia de Vega)

ABSTRAK

Nama : Lia de Vega

Program Studi : Kriminologi

Judul : Analisa Risiko Kualitatif Studi Kasus Pada PT "X" Perusahaan Penyedia Jasa Data Center

Semakin meningkatnya kebutuhan akan pengamanan data menyebabkan tingginya permintaan akan data center. Sebagai penyedia jasa layanan data center dengan nilai kontrak yang tidak sedikit perusahaan penyedia jasa layanan data center sepatutnya mengadakan analisa risiko dalam upaya mengurangi pencurian data. Penelitian ini melihat PT "X" sebagai penyedia jasa data center melakukan analisa risiko kualitatif. Penelitian ini menggunakan metode kualitatif, dengan wawancara dan observasi sebagai teknik mengumpulkan data. Hasil penelitian ini menemukan bahwa PT "X" belum melakukan analisa risiko dengan melewati tahapan yang baik, masih banyak kebijakan operasional yang diambil berdasarkan common sense dari manajemen

Kata Kunci: Analisa Risiko, Data Center, Colocation, Server, Rack, Keamanan Data

ABSTRACT

Name : Lia de Vega

Program of Study : Criminology

Title : Risk Analysis Case Study of PT “X” as a Data Center Service Provider

The increasing need for data security have led to higher demand for data center. As a provider of data center services with a high of contract value, a data center service provider should conduct the risk analysis in an effort to reduce the risk of data theft. The research had observed PT "X" as the provider of data center perform qualitative risk analysis. This study uses qualitative methods, with interviews and observation as a technique to collect data. The results of this study found that PT "X" has not done the risk analysis with a good pass through, there are still many operational policies taken under the common sense of management.

Key Word: Risk Analysis, Data Center, Colocation, Server, Rack, Data Security.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi dewasa ini telah memberikan perubahan kepada banyak bidang kehidupan, perkembangan teknologi juga menyebabkan media penyimpanan data tidak dilakukan dalam bentuk kertas, namun data-data tersebut disimpan dalam bentuk file, didalam media elektronik seperti harddisk, cd dan dvd. Karena perkembangan teknologi menyebabkan dewasa ini organisasi sangat bergantung kepada akses terhadap data untuk operasional sehari-hari. Selain karena tenaga yang cukup tinggi yang dibutuhkan oleh computer personal, sehingga sebuah organisasi semakin bergantung akan kebutuhan pemusatan data,konsistensi data dan kualitas data. Dengan pertambahan volume data-data penting dalam bidang finansial, global, institusi dan organisasi pemerintahan, data center semakin berevolusi menjadi kunci dari keberlangsungan oprasional sebuah organisasi. (Tarek Saadawi:2011,183). Data yang memiliki nilai informasi bagi sebuah organisasi sangatlah penting hingga melebihi nilai dari perangkat dimana data tersebut disimpan, oleh karenanya jika data tersebut rusak atau hilang hal ini akan menimbulkan kerugian finansial. Data yang disimpan juga memiliki nilai personal, budaya ataupun nilai sosial yang akan berdampak tidak hanya pada sektor finansial ketika data tersebut rusak atau hilang, karenanya kehilangan data juga sangat mungkin menyebabkan kerugian psikologis atau fisik. (Milan Petkovi´c,et all:2006,23) Untuk beberapa organisasi, sebagai contoh Rumah Sakit, keberadaan dari sebuah data menjadi hal yang sangat penting karena sangat berkaitan dengan kehidupan manusia, sedangkan untuk organisasi perbankan data merupakan hal yang sangat penting karena transaksi dilakukan hampir setiap menit sehingga data nasabah menjadi hal yang harus dijaga (Andy Jones:2005,18,187)

Sebagai ilustrasi, asumsikan bahwa database sebuah bank menyimpan data nasabah mereka, nilai tabungan dan deposito para nasabahnya. Bank tersebut

perlu menyimpan data pribadi dari nasabahnya untuk peningkatan atau penyediaan layanan baru bagi nasabahnya, oleh karena itu pemusatan data menjadi hal yang sangat penting. (Krishnamurty Muralidhar:1999,2)

Pentingnya keamanan data mendorong banyak tulisan mengenai pencurian data yang terjadi, olehnya telah banyak studi terhadap pencurian data pada sejumlah industri, seperti Retail, Makanan dan Minuman, Pelayanan Jasa Tehnologi dan Pelayanan Jasa Keuangan. Seperti yang telah dilakukan oleh *Verizone Bussiness*. Mereka memeriksa lebih dari 500 investigasi forensik yang berisi 230 juta catatan selama lebih dari empat tahun. Studi tersebut menemukan bahwa tiga perempat pencurian data berlanjut pada penyalahgunaan data hanya dalam beberapa hari. Studi tersebut juga menemukan bahwa 63% perusahaan tidak menyadari terjadinya pencurian data sampai beberapa bulan data mereka telah disalahgunakan. Lebih parah lagi, 70% dari data yang dicuri ditemukan oleh pihak ketiga, seperti para pelanggan atau bank, yang artinya kebanyakan perusahaan tidak sadar bahwa data mereka telah disalahgunakan sampai mereka mendapat peringatan dari pihak luar. Dan bahkan sampai kehilangan ditemukan, hampir setengah dari mereka membutuhkan waktu berminggu-minggu untuk membereskan masalah ini, dan hanya 37% yang berhasil membereskan dalam hitungan hari atau jam. (http://think.securityfirst.web.id)

Mengutip data CSI Institute, pada peretemuan tahunan ke-12 *Computer Crime and Security Survey*, lebih dari 60 persen hilangnya data perusahaan disebabkan ketidaktahuan pemilik perusahaan atas pencurian data yang dilakukan karyawannya sendiri. Tercatat 162 juta catatan data mengenai informasi personal telah dinyatakan hilang sepanjang tahun 2007. Jumlah ini meningkat empat kali lipat dari tahun 2006 sebelumnya yang hanya 49 juta kasus. Beberapa motivasi karyawan sampai mencuri atau membobol data rahasia perusahaan antara lain kepentingan bisnis, yakni menjual informasi itu kepada perusahaan lain. Motivasi lain karena "sakit hati" dan kecewa atas perlakuan pimpinan perusahaan. Juga saat keluar dari perusahaan itu sekalian mencuri data dan menjualnya kepada perusahaan lain. Piranti yang menjadi media pencurian antara lain melalui

personal komputer, jaringan internet, e-mail, back up data, flash disc, dan secara manual, yakni pencurian dokumen kertas tertulis (www.kompas.com)

Produsen *software* sekuriti Symantec Corp juga telah memperingatkan perusahaan-perusahaan di dunia agar mewaspadai karyawan yang meninggalkan perusahaan, entah karena PHK (Pemutusan Hubungan Kerja) atau karena mengundurkan diri. Sebab, survei Symantec mengungkap, sebanyak 59% mantan karyawan mengaku pernah mencuri data saat meninggalkan perusahaan. Sebagian besar data yang dicuri adalah data rahasia perusahaan. Misallnya data daftar kontak pelanggan, laporan-laporan finasial hingga catatan kinerja karyawan. Symantec menemukan, pencurian data tersebut paling banyak ditemukan di perusahaan-perusahaan finacial. Sebanyak 60% mantan karyawan yang mencuri data mengaku melakukan tindakan kriminal itu karena sakit hati terhadap perusahaan yang sempat ditempatinya.

Risiko pencurian data ini semakin meningkat karena dunia saat ini sedang dilanda gelombang PHK besar-besaran. Namun, pencurian data seperti ini sesungguhnya bisa dicegah apabila perusahaan memiliki sistem sekuriti yang memadai, ujar senior Director Symantec Corp Rob Greer. Symantec menjelaskan, pencurian-pencurian data itu dilakukan dengan cara sangat beragam. Sebanyak 53% pencurian data dilakukan dengan menyalin data ke dalam cakram optik, sebanyak 42% dilakukan dengan media penyimpanan eksternal seperti USB flash drive, dan sebanyak 38% dilakukan dengan mengirim data itu keluar perusahaan melalui attachment dalam e-mail. Ada pula pencurian data yang dilakukan secara lebih rapi, yakni dengan memasuki jaringan komputer perusahaan dari jarak jauh. Ini terjadi karena perusahaan tidak menutup akses *username* dan *password* karyawan yang sudah keluar. Dengan username dan password itu, mantan karyawan bisa masuk ke jaringan komputer perusahaan dan menyadap data. Survey yang sama mengungkap, sebanyak 82% perusahaan ternyata tidak merasa data mereka dicuri. Sebab, perusahan-perusahaan itu tidak melakukan audit terhadap dokumen elektronik karyawan yang keluar. Ini tentu membuat mantan karyawan leluasa melakukan pencurian data. (Koran harian Seputar Indonesia. Edisi: Kamis 26 Februari 2009. Halaman: Techno/36)

Seperti kasus pencurian data yang baru-baru ini terjadi yang menimpa salah satu perusahaan penyedia layanan komunikasi. Kejadian itu sendiri berawal ketika beberapa wakil Huawei melakukan rapat dengan pihak XL di Graha XL Mega Kuningan Jakarta Selatan, pada Jumat 13 Maret 2009. Salah seorang karyawan menyelinap ke ruang kerja *General Manager Network Planning,* Opbet Suwadji dan berusaha menyalin file-file di dalam folder My Document pada komputer milik Opbet ke dalam USB flash. Namun ia tertangkap basah oleh seorang karyawan XL lainnya. (www.vivanews.com)

Pentingnya keberadaan data bagi keberlangsungan sebuah organisasi maka menjadi perlu untuk menyimpan data dalam sebuah data center yang keamanannya terjaga dari berbagai ancaman kerusakan maupun pencurian. Hal ini sejalan dengan yang diamanatkan dalam pasal 40 ayat 4 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menyebutkan bahwa *Instansi atau institusi harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke data center tertentu untuk kepentingan pengamanan data. Instansi atau institusi harus membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya*.

1.2 Permasalahan

Mengingat pentingnya peranan data bagi sebuah organisasi, dan telah maraknya kasus pencurian data yang terjadi. Kerugian yang ditimbulkan karena pencurian data yang terjadi dapat berjumlah ratusan juta, karena data yang dijual tidak hanya dikonsumsi satu pihak saja melainkan dijual dengan nilai yang sangat besar. Sebagian besar data yang berhasil dicuri para peretas tidak dikonsumsi untuk keperluan pribadi, namun dijual ke komunitas bawah tanah. Raymond Goh, Director System Engineering Symante, menyatakan bahwa nilai transaksi penjualan data bisa mencapai miliaran dolar.(www.detik.com). Seperti yang telah dipaparkan sebelumnya bahwa pencurian data dapat terjadi tidak hanya dengan cara virtual *(hacking*) tetapi juga dapat dilakukan secara fisik. Pengamanan data elektronik berupa enkripsi yang sangat canggih pun akan percuma jika keamanan

fisik tidak diperhatikan. Oleh karena itu data perlu dialokasikan ke sebuah data center dalam sebuah sistem pengamanan yang baik.

Berdasarkan permasalahan tersebut akan dilakukan penelitian yang berfokus pada keamanan fisik data center. Keamanan fisik biasanya sering dilupakan dan tidak menjadi perhatian penting, sehingga hal ini dapat menjadi ancaman keamanan yang berpotensi besar pada sebuah data center. Salah satu bentuk dari upaya pengamanan data center adalah dengan melakukan analisa risiko pencurian data pada data center. Keamanan fisik pada sebuah data center menjadi sangat berkaitan dengan keamanan data dan kebijakan keamanan yang berlaku. Setelah banyaknya kejadian pencurian data yang dilakukan karena pengamanan fisiknya tidak cukup baik, hal ini harus menjadi acuan untuk menerapkan metode pengamanan data secara fisik dari berbagai risiko yang timbul, baik dari alat yang digunakan atau faktor kelalaian manusia maupun faktor alam. Seperti yang kita ketahui, bahwa data center memiliki standardisasi untuk operasionalnya, yang jika tidak dilakukan dengan baik dapat menyebabkan data rusak atau hilang. Kelalaian seperti ini dapat digunakan oleh pihak yang tidak bertanggung jawab sebagai celah untuk dapat merusak atau mencuri data tersebut.

1.3 Pertanyaan Penelitian

1. Bagaimanakah analisa risiko kualitatif yang diterapkan oleh PT ”X” dalam upaya mencegah pencurian data terhadap fisik server di data center?

1.4 Tujuan Penelitian

1..Melihat analisa risiko kualitatif yang dilakukan oleh PT ”X” dalam upaya dalam upaya mencegah pencurian data terhadap fisik server di data center

1.5 Signifikansi Penelitian

1.5.1 Signifikansi akademis

Signifikansi akademik dari penelitian ini adalah bahwa hasil penelitian ini dapat memberikan sumbangan pengetahuan dan data-data empiris bagi perkembangan

kajian kriminologi yang berbasis ilmu sosial, Penelitian ini ditujukan untuk kepentingan akademis. Penulis berharap kajian dalam penelitian ini dapat memberikan kajian tentang bagaimana melakukan analisa risiko dengan menggunakan metode kualitatif yang dapat menjadi pertimbangan peningkatan sistem pengamanan yang efektif dan efisien pada data center. Penulis juga mengharapkan agar penelitian ini dapat menjadi referensi akademis bagi penelitian-penelitian terkait yang akan dilakukan di masa-masa berikutnya.

1.5.2 Signifikansi Praktis

Penelitian ini diharapkan dapat memberikan gambaran bagaimana analisa risiko yang telah dilakukan PT ”X” dan dapat menjadi pertimbangan untuk melakukan analisa risiko dengan tahapan yang baik sehingga dapat menghasilkan rekomendasi bagi peningkatan kualitas pengamanan yang dilakukan oleh penyedia jasa data center

I.6. Sistematika Penulisan

1. Bab 1 merupakan pendahuluan, pada bab ini memuat latar belakang permasalahan, permasalahan, pertanyaan penelitian, tujuan penelitian, signifikansi akademis dan praktis penelitian dan sistematika penulisan.

2. Bab 2 merupakan tinjauan pustaka, pada bab ini memuat konsep data center,kerentanan,ancaman metode-metode analisa risiko,dan kerangka pemikiran bagaimana tahapan analisa risiko dilakukan.

3. Bab 3 merupakan metodologi penelitian, pada bab ini memuat metode penelitian, pendekatan penelitian, tipe penelitian, pemilihan informan dan teknik pengumpulan data.

4. Bab 4 merupakan profil organisasi dan kegiatan organisasi dalam menjalankan operasional data center. Peraturan-peraturan terkait mengenai data center serta data-data lain yang dibutuhkan guna keperluan analisis dan pembahasan.

5. Bab 5 merupakan analisis dan pembahasan, pada bab ini menguraikan dan

menjawab pertanyaan penelitian berdasarkan data yang dikumpulkan.

6. Bab 6 merupakan penutup, pada bab ini berisi kesimpulan, saran dan keterbatasan dari hasil penelitian dan analisa data lapang

BAB II
KAJIAN KEPUSTAKAAN

2.1 Kajian Literatur

Pengamanan server sudah dilakukan semenjak 40 tahun lalu, ketika komputer digunakan oleh pengguna yang berbeda-beda, dalam *"Risk Analysis for Information Technology*" memapaparkan tiga hal yang menjadi ancaman bagi teknologi informasi, diantaranya adalah keamanan fisik, akses fisik dan akses elektronik.

Ada dua strategi dasar untuk pengawasan dan audit system keamanan:

1.Aktif memonitor sistem kontrol yang menjadi tantangan, sebagai contoh aktif mengontrol program yang memantau prosedur pengguna logon dan mencatat kegagalan logon

2.Melihat efektifitas system pengamanan dengan kondisi simulasi, sebagai contoh mempekerjakan personil dari luar yang menyusup system pengamanan organisasi

Strategi tersebut diperlukan sebagai sebuah manajemen risiko yang harus dilakukan berdasarkan dua alasan, yakni : (1) perubahan lingkungan akan menghasilkan ancaman eksternal baru untuk aset Teknologi Informasi. (2) pengawasan keamanan dan proses audit akan mengungkap ancaman internal baru untuk aset Teknologi Informasi . Oleh karena itu, manajemen harus mengevaluasi eksposur berkala kehilangan yang mungkin dialami oleh organisasi

Selain itu, manajemen risiko juga dapat dilakukan dengan mengadopsi kebijakan dan prosedur untuk mencegah akses ilegal baik oleh orang dalam atau orang luar. Hal ini dinyatakan oleh Hoffer dan Straub dalam *"A General Additive Data Perturbation Method for Database Security"*. Dalam penelitian tersebut, diketahui bahwa orang dalam sangat berbahaya karena mereka melakukan lebih dari 75% dari semua penyalahgunaan komputer (1989). Hoffer dan Straub pada

penelitian ini berfokus pada pencegahan akses ilegal oleh orang dalam. Dengan mengutip pada penelitian lain, pencegaham akses ilegal oleh orang dalam dapat dilakukan dengan menggunakan "pengintai" yang merujuk pada suatu entitas yang berwenang untuk mengakses database dan menggunakan ini akses yang sah untuk mengumpulkan data yang tidak sah tentang data-data rahasia (Adam dan Wortmann, 1989 dalam Hoffer dan Straub, 1989).

Teknik kontrol akses sering diimplementasikan untuk memberikan agregat/ringkasan informasi tanpa mengungkapkan data individu. Meskipun teknik seperti ini dapat mencegah pengungkapan untuk beberapa jenis permintaan terhadap akses data, hal ini tidak menjamin pengungkapan yang tidak akan terjadi untuk semua jenis permintaan (Adam dan Wortmann, 1989). Ketika atribut nonconfidential ada dalam database yang digunakan, risiko pengungkapan mungkin bahkan lebih tinggi. Misalnya, dalam contoh bank, pengintai mungkin berupaya untuk memperkirakan investasi bersih luar Bank dengan menggunakan semua informasi yang tersedia yaitu, nilai-nilai terganggu Ekuitas, Saham/Obligasi, dan Kewajiban, serta nilai-nilai yang bersifat tidak rahasia di Tabungan milik nasabah.

Kemanan data juga dapat dipengaruhi oleh kualitas data. Penelitian lain berjudul "*Beyond Accuracy: What Data Quality Means to Data Consumers*" oleh Richard Y. Wang and Diane M. Strong menyebutkan bahwa kualitas data yang buruk dapat memiliki dampak sosial dan ekonomi yang besar. Wang dan Strong menemukan sebuah laporan industri yang mencatat bahwa lebih dari 60 persen dari perusahaan yang disurvei (500 ukuran sedang perusahaan dengan penjualan tahunan lebih dari $ 20 juta) memiliki masalah dengan kualitas data. Permasalahan terkait kualitas data ini, memepengaruhi akurasi data untuk memasukkan aspek-aspek lain seperti kelengkapan dan aksesibilitas. A New York Bank menemukan bahwa data dalam risiko kredit manajemen databasenya hanya 60 persen yang terselesaikan, memerlukan pemeriksaan ganda oleh siapapun yang menggunakannya. Sebuah perusahaan manufaktur besar menemukan bahwa mereka tidak dapat mengakses semua data penjualan untuk

pelanggan tunggal karena banyak nomor pelanggan yang berbeda untuk mewakili pelanggan yang sama.

Pengamanan data seperti yang ditulis oleh Roger Needham dalam penelitiannya yang berjudul "*The Clifford Paterson Lecture, 2002 Computer Security?* tidak mungkin lagi hanya menggunakan cara-cara fisik untuk mencegah akses yang tidak diperbolehkan, karena data yang diberikan dari satu tempat ke tempat lain pada media biasanya disampaikan ke mesin lain dengan internet. Unikasi membuatnya lebih sulit untuk melewatkan data yang dirancang untuk mengotentikasi individu, seperti password. Orang melihat keamanan dari berbagai cara. Mereka mungkin pengguna sistem yang membutuhkan perlindungan dari satu sama lain dan dari siapa sistem itu sendiri perlu dilindungi. Mereka mungkin orang-orang yang mengatur sistem keamanan, mereka mungkin orang-orang yang menentukan daftar hak akses, mereka mungkin menjadi administrator keamanan lokal. Oleh karena itu, menurut Needham pengamanan data perlu meliputi beberapa aspek berikut:

1. **Kerahasiaan**

   Semua teknik untuk otentikasi tergantung pada dapat diaksesnya fisik. Orang tidak bisa mengingat kunci enkripsi yang rumit, atau kode iris yang menjadi ciri mereka, misalnya. Ini harus disimpan dalam beberapa objek, dan integritas otentikasi tergantung pada integritas objek ini. Banyak objek yang tidak cocok untuk menjaga materi syang bersifat rahasia yang tidak boleh diungkapkan atau diubah. Secara khusus, komputer pribadi (PC) tidak cocok, dan mendapatkan lebih sehingga menjadi hal biasa untuk PC di rumah akan terhubung ke Internet sepanjang waktu

2. **Peraturan**

   Kebijakan keamanan organisasi yang luas, informal, dan mudah dimengerti. Tidak ada notasi yang tepat untuk mengatakan kebijakan mana yang paling tepat, dan mereka tumbuh dari waktu ke waktu.

Sumber kebijakan kadang-kadang bersumber dari apa yang dilihat sebagai 'akal sehat', dan kadang-kadang merupakan efek persyaratan hukum

3. Manusia

seringkali masalah pengamanan data disebabkan oleh faktor manusia, karena personil keamanan yang malas dan tidak mengerti prosedur pengamanan

Pada masa sekarang cara pengamanan juga telah menggunakan alat bantu dalam pengawasan dengan menggunakan CCTV sebagai alat pemantau yang terbukti dapat mengurangi tingkat kejahatan. Dalam penelitian yang membahas mengenai penggunaan CCTV oleh Brandon C. Welsh and David P. Farrington dalam jurnal yang berjudul *"Effects of Closed-Circuit Television on Crime"* disebutkan CCTV merupakan sebuah bentuk intervensi yang ditargetkan pada kejahatan, CCTV adalah salah satu jenis pencegahan kejahatan situasional (Clarke 1995). Menurut Clarke dan (1997) klasifikasi Homel tentang pencegahan kejahatan situasional, CCTV dipandang sebagai teknik "pengawasan formal." Dalam hal ini, kamera CCTV yang sengaja diperlihatkan untuk meningkatkan atau menggantikan personil keamanan. Berikut yang menjadi faktor mengapa CCTV dapat mengurangi kejahatan:

1. Tertangkap dalam tindakan pelaku akan terdeteksi dan mungkin dihapus atau dihalangi

2. Pelaku yang mengetahui bahwa dirinya telah terekam oleh CCTV akan menghalangi pelaku potensial untuk kembali melakukan karena merasakan peningkatan risiko tertangkap oleh CCTV

3. CCTV dapat menyebabkan lebih banyak orang untuk merasa aman untuk mengunjungi tempat-tempat yang diawasi oleh CCTV. Hal ini akan meningkatkan tingkat pengawasan alami oleh para pengunjung, yang dapat menghalangi pelaku potensial untuk melakukan kejahatan

4. Publikasi yang dilakukan dengan CCTV dapat menyimbolkan upaya untuk mencegah kejahatan serius, dan persepsi dari upaya tersebut dapat memberikan energi kepada warga negara untuk taat hukum dan atau mencegah kejahatan

5. CCTV dapat mengurangi waktu yang digunakan untuk melakukan kejahatan, membutuhkan perpanjangan waktu dan usaha yang lebih karena merasa telah ditertangkap oleh kamera CCTV

6. Kehadiran CCTV dapat mengingatkan orang tentang pelanggaran hukum yang telah terjadi dan mendorong orang untuk mengambil tindakan pengamanan dasar, seperti mengunci mobil mereka, dan sebagainya

7. Diduga keberadaan CCTV dapat mempermalukan orang yang melakukan kejahatan, hal ini membuat takut orang untuk melakukan pelanggaran karena mereka akan direkam oleh kamera pengawas.

Salah satu jurnal yang membahas mengenai keamanan data adalah jurnal *Notification of Data Security Breaches* yang ditulis oleh Paul M. Schwartz and Edward J. Janger. Jurnal ini mengemukakan pentingnya Hukum yang mengatur keamanan data. Dewasa ini hukum mengharuskan perusahaan swasta untuk mengungkapkan informasi untuk kepentingan konsumennya. Contoh terbaru adalah hukum salah satu Negara bagian di Amerika yang mengharuskan perusahaan untuk memberitahukan individu jika ada insiden keamanan data yang melibatkan informasi pribadi mereka. Hukum ini dibuat setelah banyak data dikemukakan mengenai banyaknya entitas data yang dilanggar dengan alas an untuk melindungi konsumen. Hukum ini mengharuskan perusahaan memberitahu konsumen tentang pelanggaran keamanan data jika hal itu terjadi. Hukum ini dibuat untuk mengeluarkan informasi jika ada kebocoroan data yang terjadi. Jurnal ini menemukan bahwa saat ini ketetapan sanksi reputasi jika hal-hal seperti ini terjadi belum lengkap. Oleh karena itu pentingnya hukum ini adalah sebagai notifikasi jika ada pelanggaran data yang dilanggar sehingga dapat dilakukan mitigasi bahaya setelah kebocoran data terjadi. Fungsi ini membutuhkan respon

multi institusi yang melibatkan beberapa institusi yang fungsinya tidak berjalan dengan baik dalam peraturan sebelumnya. Jurnal ini mendukung penciptaan alur respon yang terkoordinasi dan mengembangkan elemen-elemen pendekatan untuk menjalakan peraturan tersebut. Pusat untuk respon tersebut adalah agen respon terkoordinasi yang bertugas mengawasi langkah yang dilakukan dalam melakukan perlindungan terhadap data konsumen dan meningkatkan mitigasi jika keamanan data tersebut dilanggar. Selain itu jurnal ini juga mengemukakan bahwa badan koordinasi tersebut akan melakukan gerakan perlindungan otomatis atas nama konsumen yang dilanggar keamanan datanya. Dan pada akhirnya badan koordinasi ini akan mengatur isi dari pesan notifikasi pemberitahuan mengenai pelanggaran data yang terjadi.

Keamanan informasi juga sangat diperlukan dalam dunia usaha seperti *e-commerce* dan *online banking*, seperti yang ditulis oleh Bomil Suh and Ingoo Han dalam jurnalnya yang berjudul *" The Impact of Customer Trust and Perception of Security Control on the Acceptance ofElectronic Commerce"* Jurnal ini menginvestigasi mengenai dampak persepsi konsumen terhadap penerimaan akan kontrol keamanan pada *e-commerce*. Kepercayaan diterima sebagai faktor mediasi hubungan antara penggunaan internet banking sebagai domain melakukan pencarian, hal ini dikarenakan para konsumen bank yang umumnya khawatir tentang proses yang membutuhkan informasi sensitif seperti informasi keuangan. Sebuah survei web dari pengguna internet banking menggunakan sampel dari 502 kasus. Analisis statistik, dilakukan dengan menggunakan model persamaan struktural, analisa ini menunjukkan bahwa persepsi penyangkalan, perlindungan privasi, dan integritas data memiliki dampak yang signifikan pada kepercayaan dalam dunia *e-commerce*. Kepercayaan juga memiliki dampak yang signifikan agar konsumen mempercayakan transaksinya lewat *e-commerce*. Berdasarkan analisis tersebut terlihat bahwa manajemen pengamanan data menjadi hal yang sangat penting sebab akan berdampak langsung pada kepercayaan konsumen.

Studi mengenai kepercayaan terkait dengan pengamanan data juga dilakukan oleh Ioannis V. Koskosas and Ray J. Paul, dalam penelitian yang berjudul *Information Security Management in the Context of Goal-Setting*.

Penelitian ini menunjukkan sebuah kerangka kerja yang didasarkan pada konsep tujuan untuk mengelola keamanan informasi. Kerangka kerja ini menggambarkan perspektif sosial-organisasi seperti komunikasi kepercayaan, budaya dan risiko dalam konteks keamanan informasi. Tiga studi kasus yang dilakukan menunjukkan bukti bahwa ada reaksi berantai di antara isu-isu ini, dengan efek berikutnya pada tingkat keamanan penetapan tujuan. Artinya, kepercayaan, budaya dan komunikasi risiko memainkan peran penting di tingkat pengaturan keamanan, dan kepercayaan menyediakan kondisi di mana budaya kelompok yang kuat dan komunikasi yang efektif dari risiko yang mungkin terjadi.

Penelitian ini juga menggunakan pendekatan deskriptif-interpretatif sebagai modus penyelidikan Sebuah Model Analisis Risiko untuk Mengurangi Risiko Keamanan Komputer antara pada organisasi kesehatan. Jurnal ini menjelaskan pengembangan berkelanjutan metodologi berbasis komputer untuk melakukan analisis risiko keamanan yang dapat digunakan untuk menentukan persyaratan keamanan komputer dari sistem komputer bidang medis. Metodologi ini telah dikembangkan untuk digunakan dalam perawatan kesehatan, dengan penekanan khusus yang ditujukan untuk melindungi sistem informasi medis. Makalah ini berlanjut dengan melukiskan beberapa masalah yang ada dengan sistem analisis risiko otomatis.

Rein Turn et all dalam ”*Privacy and Security in Centralized vs. Decentralized Databank Systems”* Pemusatan Data di Amerika sudah dimulai pada tahun 1965 ketika Biro keuangan merekomendasikan bahwa layanan data center sebaiknya didirikan yang akan berisi informasi pribadi individu yang dikumpulkan untuk tujuan statistik. Sistem ini, yang akhirnya menjadi dikenal sebagai National Data Bank (NDB), menjadikan seluruh data terkomputerisasi yang hanya digunakan untuk keperluan statistik. Dalam NDB, fungsi penyimpanan data adalah ditujukan agar data benar-benar terpusat, dan integrasi dapat dilakukan dengan maksimum.

Dalam penelitian ini peneliti mengemukakan mengenai pentingnya keamanan data Keamanan data dapat dicapai dengan kombinasi dari keamanan

fisik, perangkat lunak dan akses kontrol, integritas-teknik manajemen, dan kontrol akan kesalahan. Ancaman yang diperhatikan diklasifikasikan sebagai invasi fisik yang jelas, subversi personil dan pengguna resmi, intrusi teknis dari luar, dan kerusakan sistem disengaja. Penerapan sistem data keamanan yang efektif mensyaratkan bahwa manajemenpaling atas harus sadar akan masalah keamanan dan bahwa mereka bersedia untuk (1) mengalokasikan dana yang memadai untuk menginstal mekanisme keamanan fisik, (2) membentuk manajer keamanan penuh waktu, mempekerjakan staf yang memadai, dan mengarahkan semua staf untuk menegakkan peraturan keamanan; (3) membuat program keamanan kesadaran di antara karyawan bank data, dan (4) mempekerjakan analis sistem yang sangat mampu dan programmer untuk mengimplementasikan mekanisme keamanan

Penelitian lain yang juga menulis tentang pengamanan data adalah *Law for Computer Misuse and Data Protection* oleh C. Satapathy. Pada penelitian ini, Satapathy mengemukakan bahwa Komisi Hukum Skotlandia telah mengidentifikasi delapan kategori berikut penyalahgunaan komputer: (1) penghapusan atau pemalsuan data atau program untuk memperoleh keuntungan berupa uang atau lainnya, (2) mendapat akses tanpa izin ke komputer, (3) menguping data yang ada dalam computer orang lain. (4) mengambil informasi tanpa penghapusan fisik, (5) pinjaman yang tidak sah dari disk komputer atau kaset, (6) membuat penggunaan yang tidak sah dari waktu komputer atau fasilitas, (7) korupsi berbahaya atau ceroboh atau penghapusan data atau program, dan (8) penolakan akses untuk pengguna yang berwenang. Komisi Skotlandia merasa bahwa kategori 1 dapat berdasarkan peraturan hukum Skotlandia dapat dikategorikan sebagai tindak penipuan dan pencurian, sedangkan kategori 7 dalam peraturan hukum Skotlandia dikategorikan sebagai tindak pengrusakan berbahaya dan vandalisme. Dalam penelitian ini, Satapaty juga menambahkan bahwa penyalahgunaan komputer harus diperlakukan dengan cara yang sama seperti halnya pelanggaran atau penyalahgunaan dengan peralatan lain.

2.2 Definisi Konseptual

Risiko

Risiko adalah fungsi dari ancaman dan kerentanan. Risiko adalah kemungkinan ancaman kehilangan aset, kerusakan atau kehancuran sebagai hasil dari ekspoitasi ancaman oleh kerentanan. (Karim H. Vellani 2007: 14)

Data

"*Generally, data represent a structured codification of single primary entities, as well as of transactions involving two or more primary entities* ." (Vercellis, 2009: 6).

Secara General data mewakili kodifikasi terstruktur sebuah entitas tunggal, serta transaksi yang melibatkan dua atau lebih entitas utama (Vercellis, 2009: 6).

Data center

" *A data center is a facility used for housing a large number of servers/workstations, data storages devices, communications equipment, and monitoring devices"*

Data center adalah fasilitas yang digunakan untuk menempatkan server dalam jumlah besar, penyimpanan data, peralatan komunikasi dan alat untuk monitoring. (Tarek Saadawi et all:2011,184)

Trade Secret

Menurut (Magnabosco,John 2009:19) Data korporat, atau yang dikenal dengan *trade secret* adalah rahasia dagang. Rahasia dagang merupakan aspek penting dari persaingan perusahaan, seperti kualitas, desain atau keunikan produk yang memberikan keunggulan atas produk sejenis yang berdedar dipasar

CCTV

CCTV yang merupakan singkatan dari Closed Circuit Television merupakan system televisi dengan monitor yang dapat memvisualisasikan sebuah lokasi atau kegiatan untuk tujuan pengamanan. CCTV tidak disiarkan untuk konsumen umum dan tidak menyiarkan saluran TV tetapi mentransmisikan hasil monitoring tersebut dalam bentuk digital melalui closed circuit dengan menggunakan kabel elektrik, fiber optic atau wireless transmisi (Herman Kruegle:2007,629)

Colocation

A colocation center is where multiple customers locate network, server and storage equipment which have the ability to interconnect a variety of telecommunications as well as multiple network service providers in one location with a minimum of cost and complexity

Colocation adalah tempat dimana beberapa pelanggan mengalokasikan jaringan, server dan peralatan penyimpanan yang memiliki kemampuan untuk menghubungkan berbagai jaringan telekomunikasi serta penyedia beberapa layanan jaringan dalam satu lokasi dengan biaya dan kompleksitas seminimal mungkin (Team Companies,2009:3)

2.3 Kerangka Pemikiran

2.3.1 Analisa Risiko

Analisa risiko merupakan cara managemen untuk menganalisa suatu risiko dengan cara menentukan besarnya kemungkinan/probability dan tingkat keparahan dari akibat/consequences suatu risiko. Analisa risiko dapat digunakan sebagai rekomendasi penanganan risiko yang akan dilakukan oleh manajemen. Penelitian ini ingin melihat bagaimana praktek analisa risiko yang dilakukan PT "X" karena sebagai Data center yang menyimpan banyak data krusial pelanggannya sudah pasti Data center memiliki risiko. Dalam analisa risiko

terdapat 2 jenis metode, yakni kuantitatif dan kualitatif. Kedua metode analisa ini sama-sama berguna untuk mengidentifikasi dan mengklasifikasikan tingkat ancaman yang dihadapi. (Fenelly,2004:494) Metode yang pertama adalah metode kualitatif, metode ini melibatkan beberapa cara yakni, wawancara dengan interpretasi, kalimat-kalimat dan gambar. Sedangkan metode kuantitatif melibatkan beberapa cara seperti menginterpretasi angka, dan estimasi. Secara sederhana analisa kualitatif memerlukan intuisi sedangkan kuantitatif memerlukan kemampuan matematis yang baik. Begitu juga dengan laporan yang dihasilkan, kualitatif berbentuk kata-kata yang harus dibaca secara rinci sedangkan laporan kuantitatif berisi grafik, tabel keduanya sama-sama perlu dicerna dengan baik. (Norman,Thomas,2003:5) Analisa kualitatif banyak dilakukan dalam bidang yang komplex yang seringkali lebih mudah untuk berkomunikasi dengan menggunakan analisis data kualitatif untuk audiens yang lebih luas karena analisa kualitatif memiliki kemampuan yang lebih baik untuk menggambarkan risiko secara rinci dengan contoh-contoh dalam kehidupan nyata (Jones,Andi:2005,216)

Seringkali banyak kasus yang tidak mungkin atau tidak perlu dilakukan dengan menggunakan metode kuantitatif,sehingga metode kualitatif banyak dipilih karena beberapa alasan (Yoe,Charles,2012:151)

- Untuk tugas-tugas rutin yang tidak terlalu kontroversial
- Ketika membutuhkan konsistensi dan transparansi dalam penanganan risiko
- Ketika teori, data, waktu, atau tenaga ahli terbatas
- Ketika berhadapan dengan masalah yang didefinisikan secara luas dimana analisa risiko kuantitatif tidak praktis untuk dilakukan

Sebuah proses analisa risiko kualitatif mengkompilasi, menggabungkan, dan menyajikan bukti untuk mendukung perkiraan non numerik dan deskripsi dari sebuah risiko. Dengan menggunakan metode kualitatif kita dapat mengklasifikasikan risiko ke dalam beberapa tingkat yaitu (Evan Wheeler et all:2011,68)

Tabel 2.1

Tabel klasifikasi risiko

Level	Kriteria
Rendah	Masih dalam tingkat yang dapat diterima oleh organisasi,menghasilkan kerugian finansial yang relative rendah. Hanya akan ada imbas yang kecil dalam operasional normal
Sedang	Risiko berada dalam tingkat yang lebih tinggi,namun masih dalam tingkat yang dapat diterima oleh organisasi. Namun risiko akan terasa dampaknya bagi operasional organisasi dan akan menyebabkan palanggaran pada kewajiban yang harus dilakukan oleh para karwayan.
Tinggi	Pada level ini risiko tidak dapat diterima, karena risiko dalam tingkat ini menghasilkan kerugian finansial yang tinggi dan dapat mengancam reputasi organisasi. Kemampuan organisasi untuk melaksanakan operasional akan sangat terganggu, risiko dalam tingkat ini juga akan menyababkan ketidak percayaan akan aturan yang berlaku dan akan menyebabkan hilangnya kepercayaan publik akan organisasi.

(Sumber: Evan Wheeler et all:2011,68)

Data dan analisis numerik dapat menjadi bagian dari masukan untuk penilaian risiko kualitatif, tetapi bukanlah menjadi bagian dari output karakterisasi risiko. Analisa risiko kualitatif menghasilkan paparan deskriptif atau kategorikal informasi mengenai risiko Sedangkan analisa kuantitatif bergantung pada ekspresi numerik risiko dalam karakterisasi yang dimiliki risiko tersebut. Ukuran-ukuran numerik risiko umumnya terkadang lebih informatif daripada perkiraan kualitatif. Ketika data dan sumber daya yang memadai tersedia untuk melakukan analisa, penilaian kuantitatif lebih disukai, kecuali jika pertanyaan mengenai risiko bisa cukup dijawab dalam sebuah narasi atau laporan model kualitatif lainnya

Penilaian kuantitatif dapat deterministik atau probabilistik. Pilihan tergantung pada risiko yang akan dianalisa, data yang tersedia, sifat ketidakpastian, keterampilan para analis, efektivitas hasil analisa dalam menginformasikan dan memberikan rekomendasi kepada pengambil keputusan Umumnya, karakterisasi risiko berdasarkan metode kuantitatif mengarahkan manajemen risiko pada tingkat yang lebih detail dan memiliki resolusi yang lebih baik pula daripada penilaian risiko kualitatif. Metode ini dapat lebih rinci dalam memperkenalkan kebutuhan untuk penanganan yang lebih baik akan ketidakpastian dalam karakterisasi risiko yang sedang dihadapi daripada yang dihasilkan oleh analisa kualitatif .Berikut merupakan perbandingan analisa risiko kuantitatif dan kualitatif (Krutz and Vinez,2003:24)

Tabel 2.2

Tabel Perbedaan Analisis Risiko Kualitatif dan Kuantitaif

Point	Kuantitatif	Kualitatif
Analisa biaya/manfaat	Ya	Tidak
Biaya finansial	Ya	Tidak
Dapat diotomasikan	Ya	Tidak
Melibatkan penafsiran	Rendah	Tinggi
Melibatkan perhitungan kompleks	Ya	Tidak
Jumlah dari informasi yang dibutuhkan	Tinggi	Rendah
Waktu / Pekerjaan yang dilibatkan	Tinggi	Rendah
Kemudahan berkomunikasi	Tinggi	Rendah

(Sumber:Krutz and Vinez,2003:24)

2.3.2 Analisa Risiko Kualitatif

Dalam penelitian ini peneliti menggunakan metode analisa kualitatif sebagai bahan pertimbangan PT "X" untuk melakukan analisa risiko kualitatif dikarenakan banyaknya keterbatasan yang dimiliki oleh PT "X" yaitu:

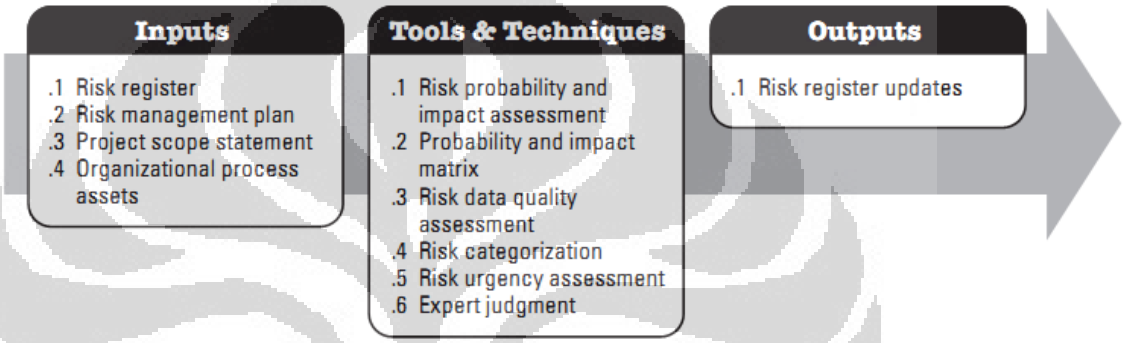
1. Tidak adanya tenaga ahli, seperti risiko analis yang dapat melakukan analisa risiko kuantitatif yang bersifat lebih kompleks
2. Tidak lengkapnya data historis mengenai kejahatan yang pernah terjadi di data center.
3. Belum mapannya proses penanganan risiko yang dibuktikan tidak adanya divisi khusus yang didelegasikan untuk menangani risiko yang dihadapi oleh PT "X".

Analisis Risiko Kualitatif adalah pengukuran risiko atau nilai aset berdasarkan peringkat atau pemisahan ke dalam kategori deskriptif seperti rendah, sedang, tinggi, tidak penting, penting, dll sangat penting atau pada skala dari 1 sampai 5. Analisis Risiko Kualitatif merupakan salah satu metode untuk membuat tingkatan prioritas risiko yang berhasil diidentifikasi untuk mendapatkan tindakan lebih lanjut, seperti Analisis Risiko Kuantitatif atau Perencanaan Respon Risiko. Organisasi dapat meningkatkan kinerja secara efektif dengan berfokus pada risiko dengan prioritas tinggi. Analisis Risiko Kualitatif menilai prioritas risiko yang berhasil diidentifikasi dengan menggunakan tingkat probabilitas risiko itu sendiri , dampak yang akan terjadi jika risiko benar-benar muncul, serta faktor-faktor lain yang mempengaruhi seperti toleransi waktu, dan risiko kendala yang dihadapi seperti biaya, jadwal, ruang lingkup dan kualitas operasional. Analisis Risiko Kualitatif biasanya merupakan cara yang cepat dan hemat biaya untuk membuat prioritas risiko sebagai bahan pembuatan Perencanaan Respon Risiko, dan menjadi dasar bagi Analisis Risiko Kuantitatif, jika ini diperlukan. Analisis risiko kualitatif membutuhkan hasil dari rerencanaan manajemen risiko dan proses Identifikasi risiko. Proses ini dapat mengarah ke analisis risiko kuantitatif atau langsung ke perencanaan respon terhadap risiko.

Tahapan analisa risiko menggunakan metode kualitatif terdiri dari beberapa tahapan, mengumpulan input yang diperlukan, lalu mengolahnya dengan beberapa pilihan strategi dan menghasilkan output berupa *risk register* yang telah diperbaharui (Project Management Institute,2008:302)

Gambar 2.1

Gambar Tahapan Analisa Risiko



(Sumber: Project Management Institute,2008:302)

2.3.3 Input Analisa Risiko

Analisis Risiko Kualitatif menilai dampak dan kemungkinan risiko yang teridentifikasi secara cepat dan dengan biaya yang kecil. Dengan mengevaluasi prioritas risiko berdasarkan pertimbangan atas biaya proyek, jadwal proyek,ruang lingkup analisa, dan sasaran mutu,maka analisa kualitatif sangatlah direkomendasikan. Analisis Risiko Kualitatif kedepannya dapat menyediakan landasan untuk melakukan analisis kuantitatif atau perencanaan respon terhadap risiko. Masukan atau bahan untuk melakukan proses Analisis Risiko Kualitatif adalah sebagai berikut:

2.3.3.1 Risk Register

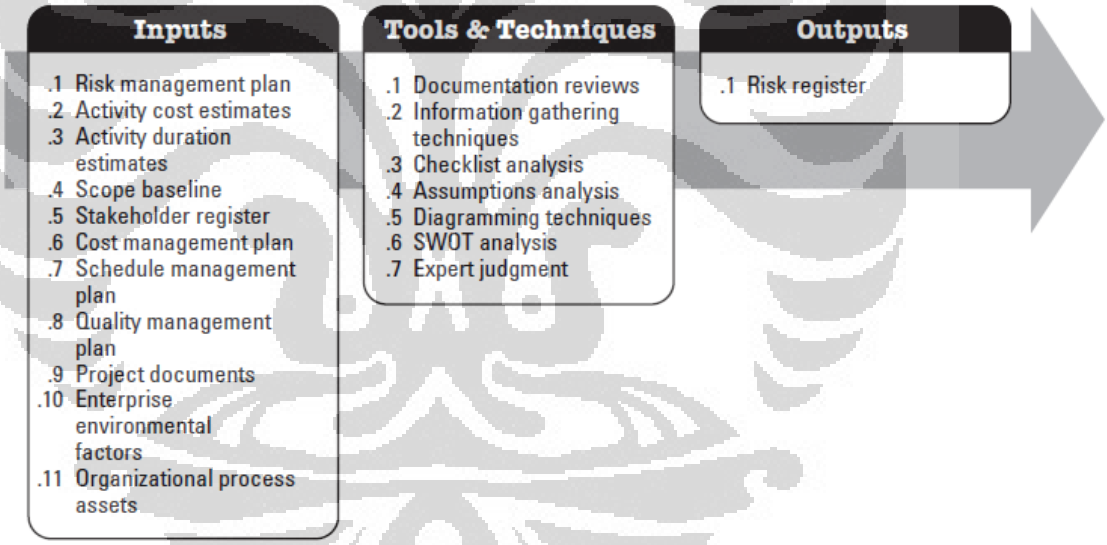
Risk register merupakan Daftar catatan Risiko yang berisi rincian semua risiko yang berhasil diidentifikasi pada awal dan selama proyek analisa berlangsung,

penilaian tersebut dilakukan dengan melihat kemungkinan yang dapat terjadi dan dampak yang ditimbulkan pada proyek (dalam hal ini pengamanan data center), risk register dibuat untuk melihat daftar risiko sehingga dapat dijadikan acuan untuk mengurangi setiap risiko dengan tingkat urgensi yang tinggi, dan dampak biaya dan tanggung jawab dari strategi mitigasi yang telah dilakukan dan hasil dari tahapan berikutnya yang diharapkan.

Berikut merupakan tahapan risk register,mengumpulkan informasi mengolahnya sehingga menghasilkan risk register (daftar risiko)

Gambar 2.2

Gambar Bagan Tahapan Membuat Risk Register



(Sumber: Project Management Institute,2008:302)

2.3.3.1.1 Risk Register Input

Dalam mengidentifikasi risiko yang ada dalam sebuah proyek, dibutuhkan beberapa input yang dapat digunakan dalam membuat daftar risiko yang dijadikan sebagai input pelaksanaan analisis risiko kualitatif, input-input tersebut antara lain: (Sumber: Project Management Institute,2008:286)

2.3.3.1.1.1 Risk Management Plan

Masukan utama dari rencana manajemen risiko untuk proses Mengidentifikasi Risiko adalah bentuk tugas dari peran dan tanggung jawab proses manajemen risiko yang dilakukan, ketentuan untuk kegiatan manajemen risiko, anggaran dan jadwal, dan kategori risiko yang dikelola dalam rencana manajemen risiko

2.3.3.1.1.1.2 Perkiraan biaya kegiatan identifikasi risiko

Review perkiraan biaya aktivitas yang akan dikeluarkan ketika menjalankan identifikasi risiko sangat berguna dalam membuat daftar risik. Karena Review tersebut dapat memberikan penilaian kuantitatif dari estimasi biaya untuk menyelesaikan kegiatan yang dijadwalkan. Idealnya perkiraan tersebut dinyatakan dalam sebuah *range*, dengan lebar rentang yang menunjukkan tingkat risiko.

2.3.3.1.1.1.3 Perkiraan jangka waktu pelaksanaan kegiatan

Review perkiraan durasi aktivitas berguna dalam mengidentifikasi risiko yang terkait dengan toleransi waktu yang diberikan oleh manajemen untuk kegiatan atau proyek secara keseluruhan, dengan lebar kisaran perkiraan tersebut menunjukkan tingkat relatif dari risiko

2.3.3.1.1.1 4 Scope Baseline

Asumsi mengenai proyek dapat dilihat dari *project scope statement.* Ketidakpastian asumsi dalam *project scope statement* harus dievaluasi sebagai penyebab risiko potensial dari proyek.

2.3.3.1.1.1.5 Stakeholder Register

Dalam mengidentifikasi risiko perlu dibuat stakeholder register yang mencakup hasil yang akan didapat oleh setiap *stakeholder,*hal ini sangat penting karena ini

akan memastikan bahwa para pemangku kepentingan, terutama pelanggan, atau pihak yang diwawancarai atau berpartisipasi selama proses identifikasi risiko berlangsung.

2.3.3.1.1.1.6 Rencana Pengelolaan Biaya

Proses identifikasi risiko membutuhkan pemahaman tentang rencana pengelolaan biaya yang dapat ditemukan dalam rencana manajemen proyek. Pendekatan proyek khusus untuk biaya manajemen dapat menghasilkan atau mengurangi risiko menurut sifat atau strukturnya

2.3.3.1.1.1.7 Schedule Management Plan

Proses identifikasi risiko juga membutuhkan rencana pengelolaan jadwal. Pendekatan proyek khusus untuk menjadwalkan manajemen dapat menghasilkan atau mengurangi risiko menurut sifat atau strukturnya

2.3.3.1.1.1.8 Rencana Pengelolaan Kualitas

Proses identifikasi risiko juga membutuhkan rencana manajemen mutu. Pendekatan proyek khusus untuk manajemen mutu yang akan dicapai oleh perusahaan dapat menghasilkan atau mengurangi risiko menurut sifat atau struktur.

2.3.3.1.1.1.9 Project Documents

Dokumen proyek termasuk, namun tidak terbatas pada:

- Catatan asumsi
- Laporan Kinerja
- Nilai-nilai yang sudah dihasilkan selama proyek berjalan

2.3.3.1.1.1.10 Faktor yang mempengaruhi perusahaan

Faktor lingkungan perusahaan yang dapat mempengaruhi proses operasional perusahaan.

2.3.3.1.1.1 11 Organizational Process Assets

Organizational proses asset meliputi semua dokumen yang dimiliki oleh perusahaan, seprti SOP, standarisasi keamanan kerja,organizational chart dan sebagainya.

2.3.3.1.2 Identify Risk process

Setelah input yang menjadi masukan dalam membuat risk register didapat maka, input tersebut dapat dioleh melalui beberapa proses yang dapat dipilih salah satunya, beberapa proses tersebut diantaranya (Sumber: Project Management Institute,2008:286)

2.3.3.1.2.1 Review dari Dokumentasi

Sebuah tinjauan terstruktur yang dapat dilakukan dengan melihat dokumentasi proyek sebelumnya, termasuk rencana, asumsi, file-file yang berkaitan dengan proyek sebelumnya, kontrak, dan informasi lainnya. Rencana pengelolaan kualitas, serta konsistensi antara rencana dan persyaratan dan asumsi proyek, hal-hal tersebut dapat menjadi indikator risiko dalam proyek

2.3.3.1.2.2 Teknik Pengumpulan Informasi

Contoh teknik pengumpulan informasi yang digunakan dalam mengidentifikasi risiko dapat termasuk:

- Brainstorming. Tujuan dari brainstorming adalah untuk mendapatkan daftar lengkap dari risiko proyek. Tim proyek biasanya melakukan brainstorming, seringkali dengan satu set multidisiplin ahli yang bukan bagian dari tim proyek internal
- Kuesioner. Seorang fasilitator menggunakan kuesioner untuk mengumpulkan ide-ide tentang risiko proyek penting.

2.3.3.1.2 3 Checklist Analisa

Identifikas daftar Risiko dapat dikembangkan berdasarkan informasi historis dan pengetahuan yang telah terakumulasi dari proyek serupa sebelumnya.

2.3.3.1.2.4 Analisa Asumsi

Setiap proyek dan setiap risiko proyek yang diidentifikasi, dapat dipahami dan dikembangkan berdasarkan sejumlah hipotesis, skenario, atau asumsi. Analisis asumsi mengeksplorasi validitas asumsi yang berlaku untuk proyek. Analisa tersebut dapat mengidentifikasi risiko terhadap proyek atas ketidaktelitian, ketidakstabilan, inkonsistensi, atau ketidaklengkapan asumsi sebelumnya.

2.3.3.1.2.5 Teknik Diagram

Teknik diagram risiko mencakup:

1. Diagram penyebab dan Efek yang ditimbulkan. Diagram ini juga dikenal dengan nama diagram Ishikawa atau fishbone
2. Sistem atau flowchart. Hal ini menunjukkan bagaimana berbagai elemen sistem saling berhubungan, dan mekanisme sebab-akibat.
3. Diagram pengaruh. Diagram ini adalah representasi grafis dari situasi yang menunjukkan pengaruh kausal, dan hubungan lain antara variabel dan hasil.

2.3.3.1.2.6 Analisa SWOT

Teknik ini meneliti proyek dari masing-masing SWOT (kekuatan, kelemahan, peluang, dan ancaman) perspektif untuk meningkatkan jumlah risiko yang telah diidentifikasi dengan memasukkan risiko internal. Teknik ini dimulai dengan identifikasi kekuatan dan kelemahan organisasi, baik organisasi berfokus pada proyek atau bisnis yang lebih luas. Faktor-faktor ini sering diidentifikasi dengan menggunakan brainstorming

2.3.3.1.2.7 .Penilaian Ahli

Risiko dapat diidentifikasi secara langsung oleh para ahli dengan pengalaman yang relevan dari proyek atau area bisnis serupa. Ahli tersebut harus diundang oleh manajer proyek untuk mempertimbangkan semua aspek proyek dan menyarankan risiko berdasarkan pengalaman sebelumnya dari bidang keahlian.

2.2.3.1.3 Hasil identifikasi Risiko

2.2.3.1.3.1 Risk Register

Hasil dari identifikasi risiko adalah risk register meliputi:

- Daftar risiko yang teridentifikasi. Risiko yang telah diidentifikasi dijelaskan secara rinci. Struktur sederhana untuk risiko yang ada dalam daftar risiko yang telah diidentifikasi dapat diterapkan, seperti peristiwa yang dapat terjadi, menyebabkan dampak, atau Jika penyebab, peristiwa dapat menyebabkan efek. Selain daftar risiko yang diidentifikasi dibuat, akar penyebab risiko tersebut mungkin menjadi lebih jelas.
- Daftar respon potensial. Potensi tanggapan untuk risiko terkadang dapat diidentifikasi selama proses mengidentifikasi risiko. Respon ini, jika diidentifikasi di proses ini, mungkin berguna sebagai masukan untuk proses rencana penanggulangan risiko

2.3.3.2 Rencana manajemen risiko

Ada beberapa bentuk strategi manajemen risiko yang dapat dilakukan oleh sebuah perusahaan (National Crime Prevention Institute:2001:48-50)

- Menghindari risiko

Cara ini dilakukan dengan menghilangkan atau memindahkan target dari risiko, sebagai contoh jika seorang penggemar koin, ia dapat menghindari risiko kehilangan dengan menyimpannya di bank, atau seorang penjual dapat mengurangi barang dagangannya di etalase toko. Namun dengan cara ini, juga

menimbulkan masalah terkait dengan penerapannya, sebagai contoh seorang yang mengurangi barangnya di etalase juga akan mengurangi pendapatannya karena pembeli kurang tertarik untuk mengunjungi tokoknya karena tidak ada contoh barang yang dipajang.

- Mengurangi risiko

Jika cara menghindari risiko tidak dapat dilakukan dapat mengatur risiko dapat dilakukan dengan cara mengurangi risiko hingga ke tahap dimana risiko tersebut masih mungkin untuk dihadapi. Contohnya sebuah toko dapat mengurangi risiko kerugian dengan cara memegang uang cash secukupnya untuk keperluan bisnis hari itu, dan langsung memindahkan uang yang didapat ke bank setiap harinya. Mengurangi risiko merupakan salah satu cara yang sering digunakan oleh banyak praktisi. Mengurangi risiko merupakan cara yang murah dan mudah untuk dilakukan dilakukan sebelum menerapkan cara yang lebih sulit dan memerlukan biaya lebih tinggi.

- Menyebarkan risiko

Metode ini melibatkan aplikasi perangkat keamanan dan prosedur dalam upaya untuk mencegah serangan kriminal, penyerang keterlambatan sehingga mereka dapat ditangkap sebelum menyelesaikan serangan, dan menolak akses ke bernilai tinggi target. Perangkat keamanan termasuk sistem penghalang, sistem pengawasan, dan sistem deteksi intrusi. Prosedur keamanan juga dilakukan untuk melindungi pegawai dan aset, serta ditujukan untuk mencegah kegagalan sistem keamanan tersebut, hal ini dilakukan dengan berbagai teknik manajemen standar seperti pengendalian persediaan yang tepat, pelatihan supervisor, akuntabilitas bagi karyawan yang berurusan dengan pembelian dan menerima, dan prosedur lain yang harus digunakan pula jika pendirian harus dikelola dengan baik

- Memindahkan risiko

Ketika risiko sudah dihindari, dikurangi dan di sebar sebanyak mungkin setelahnya cara yang dapat dilakukan adalah memindahkan risiko ke orang lain,

salah satu caranya adalah dengan menggunakan asuransi. Namun asuransi tidak akan efektif sebelum ketiga tahap sebelumnya dilakukan.

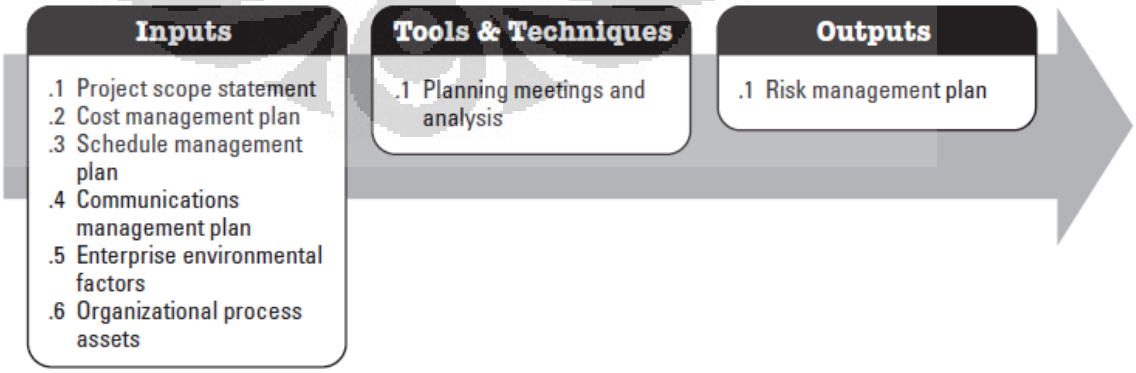
- Menerima Risiko

Setelah melakukan semua metode dalam menghadapi risiko, praktisi akhirnya harus melangkah kearah menerima risiko yang akan dihadapi. Dalam teknik ini, pengusaha atau pemilik asset harus menerima risiko residual maksimum yang mungkin menyebabkan kerugian dalam menjalankan usaha. maximum probable loss as a cost of doing business. Menerima risiko harus didukung dengan menyiapkan biayanya, menerima risiko harus dilakukan dalam tahap dimana risiko tersebut dapat diterima tanpa mengganggu operasional.

Rencana manajemen risiko menjelaskan bagaimana struktur manajemen risiko dan bagaimana akan dijalankan. Ini menjadi bagian dari rencana proyek manajemen. Rencana risiko dapat dibuat dengan melakukan tahapan seperti bagan berikut:

Gambar 2.3

Gambar Bagan Tahapan Membuat Rencana Manajemen Risiko



(Sumber: Project Management Institute,2008:277)

2.2.3.2.1 Risk Management Plan Input

Seperti halnya proses mengidentifikasi risiko yang menghasilkan risk register maka begitu juga dengan rencana pengelolaan risiko memiliki tahapan input, proses dan output. Dokumen-dokumen yang dibutuhkan untuk membuat rencana manajemen risiko antara lain: (Sumber: Project Management Institute,2008:278)

2.2.3.2.1.1 Project Scope Statement

Pernyataan lingkup proyek memberikan pandangan yang jelas tentang berbagai kemungkinan terkait dengan proyek dan hasil serta dapat menetapkan kerangka kerja untuk seberapa besar upaya manajemen risiko pada akhirnya dapat dilakukan

2.2.3.2.1.2 Cost Management Plan

Rencana pengelolaan biaya mendefinisikan bagaimana anggaran risiko, kontinjensi, dan cadangan manajemen akan dilaporkan dan bagaimana perencanaan tersebut dapat diakses oleh setiap anggota dari proyek

2.2.3.2.1.3 Perencanaan jadwal

Rencana pengelolaan jadwal mendefinisikan bagaimana jadwal kontinjensi akan dilaporkan dan dinilai. Bagaimana tenggat waktu yang akan ditetapkan untuk menjalankan proses manajemen risiko

2.2.3.1.4 Perencanaan Pengelolaan Komunikasi

Rencana pengelolaan komunikasi. Rencana ini mendefinisikan interaksi yang akan terjadi pada proyek, dan menentukan siapa yang akan siap untuk berbagi informasi mengenai berbagai risiko dan tanggapan pada waktu yang berbeda (dan lokasi).

2.2.3.1.5 Enterprise Environmental Factors

Faktor lingkungan perusahaan yang dapat mempengaruhi proses Rencana Manajemen Risiko menggambarkan tingkat risiko bahwa suatu organisasi akan bertahan.

2.2.3.1.6 Organizational Process Assets

Dokumen-dokumen yang terkait dengan proses manajemen seperti SOP, keselamatan kerja, flowchart, persyaratan finance, dan sebagainya

2.2.3.2.2 Risk Management Teknik

Untuk mengelola Input untuk rencana manajemen risiko, terdapat beberapa teknik yang dapat digunakan, diantaranya (Sumber: Project Management Institute,2008:279)

2.2.3.2.2.1 Planning Meetings and Analysis

Tim Proyek memegang merencanakan meeting untuk mengembangkan rencana pengelolaan risiko. Peserta pada pertemuan ini mungkin termasuk manajer proyek, anggota tim dipilih proyek dan stakeholder, orang dalam organisasi dengan tanggung jawab untuk mengelola risiko dan perencanaan kegiatan pelaksanaan, dan lainnya, sebagai kebutuhan. Tingkatan tingkat rencana untuk melakukan kegiatan manajemen risiko didefinisikan dalam pertemuan ini. Risiko elemen pengelolaan biaya dan jadwal kegiatan akan dikembangkan untuk dimasukkan dalam anggaran proyek dan jadwal, masing-masing. Risiko pendekatan cadangan kontingensi aplikasi dapat didirikan atau terakhir. Keluaran dari kegiatan ini akan diringkas dalam rencana manajemen risiko.

2.2.3.2.2.2 Hasil Risk Management Plan

Rencana manajemen risiko yang dihasilkan meliputi (PMBOK,2008:310):

- Metodologi: Mendefinisikan pendekatan, peralatan, dan sumber data yang dapat digunakan untuk melakukan manajemen risiko pada proyek.

- Peran dan tanggung jawab. Mendefinisikan arah proyek, dukungan bagi anggota tim manajemen risiko untuk setiap jenis kegiatan dalam rencana manajemen risiko, dan menjelaskan tanggung jawab mereka
- Penganggaran. Memberikan sumber dana, perkiraan dana yang dibutuhkan untuk manajemen risiko untuk dimasukkan dalam baseline biaya kinerja
- Waktu. Mendefinisikan kapan dan seberapa lama proses manajemen risiko akan dilakukan, dan menetapkan kegiatan manajemen risiko untuk dimasukkan dalam jadwal proyek manajemen
- Kategori Risiko. Menyediakan struktur yang menjamin proses yang komprehensif mengenai cara mengidentifikasi risiko ke tingkat yang lebih konsisten dan memberikan kontribusi terhadap efektivitas dan kualitas proses identifikasi Risiko

2.3.3.3 Project Scope Statement

Project scope statement berisi detail dari tujuan proyek, hasil yang akan terwujud, asumsi, kendala, jadwal, anggaran, dan persyaratan konfigurasi dari manajemen . *Project scope statement* menjelaskan, secara rinci, penyampaian proyek dan tindakan yang diperlukan untuk menyampaikan setiap proses yang dilakukan. *Project scope statement* juga memberikan pemahaman umum dari ruang lingkup proyek diantara para *stakeholder* proyek. *Project Scope statement* mungkin saja berisi pengecualian dari ruang lingkup yang dapat membantu dalam mengelola ekspektasi stakeholder. Ini memungkinkan tim proyek untuk melakukan perencanaan yang lebih rinci, menjadi panduan bagi kerja tim proyek, dan menyediakan dasar untuk mengevaluasi apakah permintaan untuk perubahan atau pekerjaan tambahan yang terkandung dalam atau di luar batas proyek. Tahapan membuat Project Scope Statement adalah dengan mengumpulkan input berupa project charter, dokumentasi, dan asset proses. Untuk mengolah input ini, menggunakan teknik analisa berupa penilaian ahli, analisa terhadap produk, identifikasi alternative dan workshop. Hasil dari analisa ini akan menghasilkan *Project Scope Statement.* Tahapan membuat *Project Scope Statement* seperti yang dijelaskan pada gambar bagan berikut ini

Gambar 2.4

Gambar Bagan Tahapan *Project Scope Statement.*

(Sumber: Project Management Institute,2008:112)

2.2.3.3.1 *Project Scope Statement Input*

Dokumen-dokumen yang dijadikan input dalam membuat project scope statement antara lain: (Project Management Institute,2008:113)

2.2.3.3.1.1 Project Charter

Project Charter memberikan deskripsi tingkatan tinggi proyek dan karakteristik produk. Hal ini juga berisi persyaratan persetujuan proyek. Jika sebuah project charter tidak digunakan dalam perusahaan, maka informasi yang sebanding perlu diperoleh atau dikembangkan, dan digunakan sebagai dasar untuk *project scope statement*.

2.2.3.3.2 Project Scope Statement Teknik

Input dalam project scope statement diolah dengan menggunakan beberapa cara yang dapat dipilih sesuai dengan ketersediaan data yang dimiliki oleh perusahaan (Project Management Institute,2008:114)

2.2.3.3.2.1 Expert Judgment

Penilaian pakar ini sering digunakan untuk menganalisis informasi yang dibutuhkan untuk mengembangkan *project scope statement*. Penilaian tersebut diterapkan untuk semua rincian teknis. Keahlian tersebut disediakan oleh kelompok atau individu dengan pengetahuan khusus atau dapa didapat lewat pelatihan yang tersedia dari berbagai sumber, termasuk:

- Unit lain dalam organisasi
- Konsultan
- Pemangku kepentingan, pelanggan, atau sponsor
- Profesional atau asosiasi teknik

2.2.3.3.2.1.2 Analisa Produk

Untuk proyek yang memiliki produk sebagai hasil yang harus dicapai deliverable, sebagai lawan dari layanan atau hasil, analisis produk dapat menjadi alat yang efektif. Setiap bidang aplikasi memiliki satu atau lebih metode yang berlaku umum untuk menerjemahkan tingkat tinggi deskripsi produk ke dalam hasil yang nyata. Analisis produk meliputi teknik seperti kerusakan produk, analisis sistem, analisis kebutuhan, rekayasa sistem, rekayasa nilai, dan analisis nilai dari produk tersebut

2.2.3.3.2.1.2.3 Organizational Process Assets

- Kebijakan, prosedur, dan template untuk *project scope statement*
- Proyek file dari proyek-proyek sebelumnya
- Hal-hal yang dapat dipelajari dari proyek sebelumnya

2.2.3.3.3 Hasil pendefinisian cakupan

2.2.3.3.3.1 Project Scope Statement

Pernyataan lingkup proyek menjelaskan, secara rinci, hasil dari proyek dan pekerjaan yang diperlukan untuk membuat hasil tersebut dapat dicapai. Pernyataan lingkup proyek juga memberikan pemahaman umum dari ruang

lingkup proyek antara para pemangku kepentingan proyek. Ini mungkin berisi pengecualian lingkup eksplisit yang dapat membantu dalam mengelola ekspektasi pemangku kepentingan. Ini memungkinkan tim proyek untuk melakukan perencanaan yang lebih rinci, memandu kerja tim proyek selama eksekusi, dan menyediakan dasar untuk mengevaluasi apakah permintaan untuk perubahan atau pekerjaan tambahan yang terkandung dalam atau di luar batas proyek.Project Scope Statement mencakup:

- Product scope description.
  menguraikan karakteristik produk, jasa, atau hasil dalam project charter dan dokumentasi persyaratan
- Product acceptance criteria.
  Mendefinisikan proses dan kriteria untuk menerima produk yang telah selesai, jasa, atau hasil yang akan dicapai
- Project deliverables.
  Mencakup output yang terdiri dari produk atau layanan proyek, serta hasil tambahan, seperti laporan manajemen proyek dan dokumentasi. Hasil dapat digambarkan pada tingkat ringkasan atau dengan sangat rinci.
- Daftar pengecualian proyek. Umumnya mengidentifikasi apa yang dikecualikan sebagai dari proyek tersebut. Secara eksplisit menyatakan apa yang keluar dari ruang lingkup untuk proyek membantu untuk mengelola harapan dari pemangku kepentingan
- Kendala proyek. Daftar yang menjelaskan kendala proyek secara spesifik yang terkait dengan ruang lingkup proyek yang dapat membatasi kerja tim, misalnya, anggaran yang telah ditetapkan atau tanggal yang ditetapkan atau tenggat jadwal yang dikeluarkan oleh pelanggan. Ketika proyek dilakukan di bawah kontrak, ketentuan kontrak umumnya akan menjadi kendala. Informasi tentang kendala mungkin tercantum dalam pernyataan lingkup proyek atau dalam daftar yang terpisah.
- Asumsi Proyek. Daftar dan penjelasan asumsi proyek spesifik yang terkait dengan ruang lingkup proyek dan dampak potensial dari asumsi-

asumsi jika asumsi tersebut terbukti salah. Tim proyek sering mengidentifikasi, mendokumentasikan, dan memvalidasi asumsi sebagai bagian dari proses perencanaan mereka. Informasi tentang asumsi mungkin tercantum dalam pernyataan lingkup proyek atau dalam daftar yang terpisah.

2.3.3.4 Organitional Process Assets

Organitional Process Assets mencakup salah satu atau semua proses terkait dengan aset, dari salah satu atau semua organisasi yang terlibat dalam proyek dalam hal ini pengamanan data center yang dapat digunakan untuk mempengaruhi keberhasilan proyek. *Organitional Process Assets* ini mencakup rencana formal dan informal, kebijakan, prosedur, dan pedoman. *Organitional Process Assets* juga termasuk basis pengetahuan organisasi seperti informasi historis. *Organitional Process Assets* mungkin termasuk jadwal selesai, data risiko, dan data nilai yang diterima. Memperbarui dan menambah *Organitional Process Assets* yang diperlukan sepanjang proyek umumnya tanggung jawab anggota tim proyek. *Organitional Process Assets* dapat dikategorikan kedalam dua kategori:

1. **Proses dan Prosedur:**

Standar operasional prosedur seperti, kebijakan (misalnya, keamanan dan kebijakan kesehatan, kebijakan etika, dan kebijakan manajemen proyek), standar produk dan siklus hidup proyek, dan kebijakan mutu dan prosedur (misalnya, proses audit, target perbaikan, daftar, dan standar proses definisi untuk digunakan dalam organisasi)

- Standar pedoman, instruksi kerja, kriteria usulan evaluasi, dan kriteria pengukuran kinerja

- Template (misalnya, rincian struktur kerja, proyek diagram jadwal jaringan, dan template kontrak);

- persyaratan komunikasi (misalnya, teknologi komunikasi khusus yang tersedia, media komunikasi diizinkan, kebijakan catatan retensi, dan persyaratan keamanan)

- prosedur pengawasan keuangan (misalnya, waktu pelaporan, pengeluaran yang diperlukan dan ulasan pencairan, kode akuntansi, dan ketentuan kontrak standar)

- mengubah prosedur pengawasan, termasuk langkah-langkah standar perusahaan, kebijakan, rencana, dan prosedur atau dokumen proyek akan dimodifikasi, dan bagaimana perubahan akan disetujui dan disahkan;

- Prosedur untuk memprioritaskan, menyetujui, dan penerbitan otorisasi kerja

2 Pengetahuan Dasar mengenai perusahaan

- Proses pengukuran database yang digunakan untuk mengumpulkan dan membuat data pengukuran yang tersedia pada proses dan produk
- Proyek file (misalnya, ruang lingkup, acuan dasar pengukuran biaya, jadwal, dan kinerja, kalender proyek, diagram jadwal proyek jaringan, risk register, tindakan respon terencana, dan dampak risiko yang telah ditentukan),
- Informasi historis (misalnya, proyek catatan dan dokumen, semua penutupan proyek informasi dan dokumentasi, informasi tentang hasil proyek sebelumnya dan informasi kinerja proyek sebelumnya, dan informasi dari upaya manajemen risiko),

- Masalah dan database mengenai kekurangan manajemen yang berisi masalah dan status kekurangan tersebut, informasi kontrol, solusi dari masalah sebelumnya dan hasil tindakan respon terhadap masalah

- Konfigurasi pengetahuan dasar mengenai manajemen yang berisi versi dan acuan dasar dari semua standar resmi perusahaan, kebijakan, prosedur, dan dokumen proyek

- Database keuangan yang mengandung informasi seperti jam kerja, biaya yang dikeluarkan, anggaran dan biaya proyek melebihi anggaran apapun.

2.3.4 Teknik Analisa Risiko

Setelah mengumpulkan semua masukan tahap selanjutnya adalah melakukan analisis risiko kualitatif. Ada beberapa praktik terbaik yang dapat digunakan untuk menganalisa dan memprioritaskan risiko proyek secara cepat dan efisien berdasarkan input yang telah didapat. Teknik-teknik tersebut antara lain:

2.3.4.1 Risk probability and impact assessment

Penilaian probabilitas risiko, menyelidiki kemungkinan terjadinya sebuah risiko. Penilaian dampak risiko melihat efek potensial dan dampak pada tujuan proyek seperti jadwal, kualitas biaya, atau kinerja, termasuk efek negatif untuk ancaman dan efek positif bagi peluang. Probabilitas dan dampak dinilai untuk setiap risiko yang berhasil diidentifikasi. Risiko dapat dinilai dalam wawancara atau pertemuan dengan orang-orang yang dipilih berdasarkan keterlibatan mereka dengan area risiko. Anggota tim proyek dan, mungkin, orang yang memiliki pengetahuan yang cukup mengenai proyek yang disertakan. Tingkat probabilitas untuk setiap risiko dan dampaknya terhadap masing-masing tujuan dievaluasi selama wawancara atau pertemuan. Penjelasan rinci, termasuk asumsi membenarkan tingkat yang ditetapkan, juga dicatat. Risiko probabilitas dan dampak dinilai sesuai dengan definisi yang diberikan dalam Rencana manajemen risiko yang telah dibuat. Risiko dengan probabilitas dan dampak yang rendah akan dimasukkan pada daftar pantauan untuk monitor secara rutin dimasa depan.

Tabel 2.3

Risk probability and impact assessment

Dampak	Tingkat Probabilitas
Dapat diabaikan	Rendah 0-10%
Minor	Sedang 16-29%
Sedang	Medium 30-50%
Siknifikan	Tinggi 60-79%
Kritis	Sangat tinggi,lebih dari 80%

(Sumber: Heldman,Kim:2008,255)

2.3.4.2 Matriks Probabilitas dan Dampak Risiko

Matriks probabilitas dan dampak risiko, menggambarkan rating risiko yang identifikasi. Setiap risiko dinilai berdasarkan probabilitas dan dampak terhadap tujuan proyek. Risiko dapat diprioritaskan yang dapat dijadikan acuan pelaksanaan analisis kuantitatif lebih lanjut dan respon yang akan dilakukan berdasarkan rating risiko. Biasanya,tingkat risiko ditentukan oleh organisasi dan disajikan sebagai *Organization Asset Process*. Aturan mengenai tingkatan risiko dapat disesuaikan berdasarkan proses Rencana Manajemen Risiko. Evaluasi mengenai probabilitas dan dampak dari setiap risiko dilakukan menggunakan matriks probabilitas dan dampak yang menentukan kombinasi probabilitas dan dampak yang mengarah pada rating risiko terendah, prioritas sedang, atau tinggi Dari hasil analisis warna merah menggambarkan risiko berada di zona berisiko tinggi, kuning adalah risiko sedang, dan hijau risiko dinilai rendah yang hanya harus ditambahkan ke daftar risiko yang harus dipantau.

Tabel 2.4

Matriks Probabilitas dan Dampak Risiko

Probability	**Ancaman**	**Kesempatan**

0.900	0.045	0.090	0.180	0.360	0.720	0.720	0.360	0.180	0.090	0.045
0.700	0.035	0.070	0.140	0.280	0.560	0.560	0.280	0.140	0.070	0.035
0.500	0.025	0.050	0.100	0.200	0.400	0.400	0.200	0.100	0.050	0.025
0.300	0.015	0.030	0.060	0.120	0.240	0.240	0.120	0.060	0.030	0.015
0.100	0.005	0.010	0.020	0.040	0.080	0.080	0.040	0.020	0.010	0.005
	0.050	0.100	0.200	0.400	0.800	0.800	0.400	0.200	0.100	0.050

(Sumber:anticlue.net)

2.3.4.3 Penilaian Kualitas Data Risiko

Sebuah analisa risiko kulitatif perlu memiliki data yang objektif dan akurat untuk kredibilitas analisa risiko tersebut. Sebuah penilaian kualitas data risiko merupakan sarana untuk mengevaluasi keandalan dan keakuratan informasi dari mana peringkat risiko ini berasal.

1. **Sejauh mana risiko tersebut dipahami** - Seberapa baik data mengenai risiko untuk dapat dipahami secara mendalam melalui intuisi atau empati? Data harus jelas, ringkas dan mudah dijelaskan.
2. **Ketersediaan data** – Apakah data lengkap? Cara paling umum adalah dengan mendasarkan peringkat risiko pada data yang tidak lengkap.
3. **Kualitas data** - Apakah data yang didapat tepat waktu dan relevan? Jujur mengevaluasi risiko oleh data yang 20 tahun merupakan tindakan yang tidak baik. Kebanyakan memang informasi yang ada tidak tepat waktu dan tidak relevan.
4. **Integritas dan kehandalan data** – Apakah data tersebut objektif? Analisis Risiko Kualitatif adalah analisa yang tidak pasti; Pengklasifikasian tersebut mencerminkan pendapat dan penilaian subjektif .

2.3.4.4 Penilaian Urgensi Risiko

Risiko yang membutuhkan tanggapan yang cepat merupakan risiko yang memiliki tingkat urgensi lebih tinggi. Risiko-risko yang membutuhkan respon dengan cepat mungkin dianggap lebih mendesak untuk segera diatasi. Indikator prioritas dapat mencakup waktu untuk memberikan respon kepada risiko yang muncul, gejala dan tanda-tanda peringatan, dan peringkat risiko.Dalam beberapa analisa kualitatif penilaian terhadap tingkat urgensi risiko dapat dikombinasikan dengan rating risiko yang ditentukan berdasarkan matrix kemungkinan dan dampak yang ditimbulkan

2.3.4.5 Kategorisasi Risiko

Risiko dapat dikelompokkan dengan cara yang berbeda misalnya risiko dapat dikategorikan berdasarkan sumber, daerah yang terkena dampak risko, atau fase proyek. Kategori ini menyediakan struktur yang menjamin proses yang komprehensif dan sistematis untuk mengidentifikasi risiko ke tingkat sehingga memberikan kontribusi terhadap efektivitas dan kualitas dalam proses analisa risiko. Perusahaan dapat menggunakan kerangka kategorisasi yang telah disiapkan sebelumnya, kerangka kategori tersebut mungkin mengambil daftar sederhana kategori atau mungkin terstruktur ke dalam *Risk Breakdown Structure* (RBS). RBS adalah gambaran hirarki dari risiko proyek yang berhasil diidentifikasi yang diatur berdasarkan kategori risiko dan subkategori yang mengindetifikasi berbagai bidang dan penyebab risiko potensial. Contoh *Risk Breakdown Structure* dapat dilihat pada tabel

2.3.4.6 Penilaian Ahli

Penilaian Ahli, diperlukan untuk menilai probabilitas dan dampak dari setiap risiko untuk menentukan lokasi dalam matriks probabilitas dan dampak yang ditimbulkan. Para ahli umumnya adalah mereka yang memiliki pengalaman dengan proyek serupa yang terjadi di masa lalu dengan rentang waktu yang tidak terlalu jauh. Selain itu, mereka yang merencanakan dan mengelola proyek tersebut secara spesifik, terutama tentang cs spesifik dari proyek itu. Penilaian

keamanan sering dicapai dengan penggunaan fasilitasi workshop tempat menganalisa risiko atau wawancara.

2.3.5 Hasil dari Analisa Risiko Kualitatif

Output dari proses Analisis Risiko Kualitatif adalah *Risk Register* yang telah diperbarui. Perbaharuan *risk register* meliputi:

1. **Peringkat relatif atau prioritas risiko proyek** - Peringkat risiko secara keseluruhan ditentukan dengan menjumlahkan skor masing-masing risiko dan kemudian membaginya dengan banyaknya risiko.
2. **Risiko dikelompokkan berdasarkan kategori** - Menempatkan risiko dalam kategori berdasarkan area konsentrasi risiko dan penyebab umum risiko tersebut. Misalnya, jika risiko berada diarea yang kurang memiliki sumber daya untuk menanganinya, maka mungkin perlu untuk merencanakan proyek dengan ketersediaan sumber daya yang diperlukan.
3. **Daftar risiko yang memerlukan respon dalam waktu dekat** - Risiko paling mendesak umumnya memerlukan penanganan dalam waktu dekat. Dengan menyortir risiko berdasarkan urgensi, hal ini memudahkan untuk mengidentifikasi kejadian risiko yang paling parah yang memerlukan tindakan cepat
4. **Daftar risiko untuk analisis dan respon tambahan** - Risiko yang perlu analisis tambahan dan manajemen lebih lanjut diklasifikasikan sebagai risiko yang tinggi
5. **Daftar pengawasan untuk risiko dengan prioritas rendah** - Risiko yang tidak mendesak dan memerlukan tindakan lebih jauh dimasa datang biasanya dijelaskan cesara detail dalam daftar tersebut.
6. **Tren dari hasil analisis risiko kualitatif** - Dengan setiap iterasi dari Analisis Risiko Kualitatif, tren dapat menghasilkan daftar risiko yang memerlukan respon atau analisis lebih lanjut.

BAB III

METODE PENELITIAN

3.1 Pendekatan Penelitian

Dalam penelitian ini, yang dimaksud dengan pendekatan penelitian adalah suatu strategi yang dipilih oleh peneliti untuk mengamati, mengumpulkan informasi dan untuk menyajikan analisis hasil penelitian. Untuk menggali informasi mengenai bagaimana proses manajemen risiko yang dilakukan PT. "X" dalam mengurangi risiko penulis menggunakan pendekatan kualitatif. Sejak diperkenalkan di Indonesia pada 1970-an, pendekatan kualitatif dalam penelitian terus berkembang dan mendapatkan tempat dalam dunia penelitian. Paradigma penelitian dengan menggunakan metode kualitatif pada studi ilmu-ilmu sosial saat ini menjadi sangat dominan, karena berbagai permasalahan di lapangan yang mengiringi implementasi penelitian terus bertambah dan mulai beragam. Dan mengapa hal ini menjadi demikian? Karena dapat dipahami bahwa temuan-temuan data dan fakta dalam studi dengan menggunakan pendekatan metode kualitatif, dirasakan lebih menjawab persoalan sebenarnya daripada hanya sekedar melihat statistik angka angka hasil rumusan pendekatan kuantitatif.(Burhan Bungin:2003,v)

Dalam paradigma penelitian kualitatif sangat menekankan sekali pada manfaat dan proses pengumpulan informasi-informasi secara mendalam, terutama terhadap fenomena permasalahan yang diteliti. Sehingga pendekatan penelitian kualitatif tidak hanya menekankan pada gambaran angka-angka yang mendeskripsikan

suatu permasalahan, tetapi lebih itu memberikan informasi dan gambaran mengenai suatu fenomena permasalahan tertentu. (Koentjaraningrat:1997,7) Menurut Ronny Kountur, penelitian kualitatif adalah penelitian yang datanya berupa narasi atau ilustrasi. Penelitian kualitatif pada umumnya dilakukan karena kurangnya teori-teori yang berhubungan dengan penelitian yang dilakukan, atau dikarenakan penelitian tersebut akan lebih dalam jika diinterpretasikan lewat data yang bersifat ilustrasi atau narasi. Selain itu menurut Kountur salah satu ciri penelitian kualitatif adalah tidak dapat digeneralisasikan (menarik kesimpulan secara umum) atau dengan kata lain hasil penelitian kualitatif tidak berlaku secara umum karena setiap kasus pasti memiliki keunikan. (Kountur, 2003,16-29). Penelitian kualitatif adalah salah satu tradisi dalam ilmu pengetahuan sosial yang secara fundamental bergantung pada pengamatan pada manusia dalam kawasannya sendiri dan berhubungan dengan orang-orang. penggunaan penelitian didasarkan atas pertimbangan keefektifan dari pendekatan ini dengan mengungkap peristiwa atau fenomena yang ada.

Ada beberapa alasa menggunakan menggunakan metode kualitatif, yaitu:

1. Menyesuaikan metode kualitatif lebih mudah apabila dihadapkan dengan realita yang jamak
2. Dapat menyajikan secara langsung hakikat hubungan antara peneliti dan responden
3. Metode ini lebih peka dan lebih dapat menyesuaikan diri dengan banyak pola yang dihadapi

Peneliti memilih menggunakan pendekatan kualitatif karena peneliti ingin mengetahui secara lebih mendalam mengenai pelaksanaan analisa risiko sebagai upaya mengurangi risiko pencurian data pada PT "X". Penelitian ini dilakukan berdasarkan pertanyaan penelitian yaitu Bagaimana analisa risiko kualitatif yang dilakukan oleh PT "X". Untuk menjawab pertanyaan ini, dilaksanakan penelitian dengan pendekatan kualitatif. Penelitian dengan menggunakan pendekatan kualitatif dipilih agar permasalahan dalam penelitian ini dijelaskan secara detail. Data dalam penelitian ini didapat melalui wawancara, studi

kepustakaan dan observasi, agar informasi dapat tergali secara luas dan mendalam. Hasil wawancara dan observasi tersebut akan dijelaskan melalui penjabaran informasi secara rinci

3.2 Lokasi Penelitian

Penelitian ini berlokasi disalah satu data center pada perusahaan yang menyediakan layanan data center, peneliti memilih data center ini sebagai lokasi penelitian karena berada digedung yang bukan ditujukan untuk penempatan data center, bersama dengan kegiatan oprasional kantor. Selain karena keunikan lokasi data center, banyak perusahaan terkemuka yang mempercayakan datanya kepada data center ini, sehingga pengamanan data yang dilakukan haruslah memadai karena jika tidak maka kerugian yang ditimbulkan akan sangat besar.

3.3 Tipe Penelitian

Yang dimaksud dengan tipe penelitian adalah suatu pilihan model penelitian yang mampu memberikan gambaran secara menyeluruh tentang tujuan penelitian yang hendak dicapai. Tipe penelitian yang digunakan merupakan tipe penelitian deskriptif. Sebagaimana sifat dari penelitian kualitatif, penelitian ini memiliki dua tujuan utama, yaitu pertama,menggambarkan dan menjelaskan (to describe and explain) kebanyakan penelitian. kebanyakan penelitian kualitatif bersifat deskriptif dan eksplanatori. beberapa penelitian memberikan deskripsi situasi fenomena yang diteliti dan dapat memberi arah bagi penelitian selanjutnya.

Penelitian deskriptif adalah penelitian untuk membuat pencandraan secara sistematis, faktual, dan akurat mengenai fakta-fakta dan sifat populasi tertentu. (Sumadi Suryabrata:2000,74) Mengingat tujuan penelitian ini adalah mendeskripsikan mengenai risiko pencurian data yang dihadapi oleh PT X ,serta mendeskripsikan bagaimana pengamanan yang dilakukan pada data center maka Penelitian ini bertipe penelitian deskriptif. Dalam penelitian ini peneliti berusaha untuk mendeskripsikan risiko apa saja yang terdapat dalam operasional data

center yang dimiliki oleh PT.X yang dapat menyebabkan pencurian data terjadi. Kebijakan apa yang telah dibuat dan dijalankan dalam upaya mengamankan data center. Setelah melihat kebijakan yang telah dijalankan peneliti akan mencoba mendeskripsikan bagaimana kebijakan tersebut dijalankan, dan apakah kebijakan tersebut efektif dalam mengurangi risiko pencurian data yang ada dalam gedung data center. Jika dilihat dari periode melakukan penelitian, penelitian ini merupakan *cross sectional research* karena mengambil setting waktu tertentu. Peneliti akan mengambil waktu 3 bulan untuk mengamati proses manajemen risiko yang dilakukan PT.X dalam menjalankan jasa penyedia data center. Berdasarkan waktu penelitian, penelitian ini merupakan penelitian berjenis *Cross Sectional* penelitian yang mengambil jangan waktu tertentu dalam jangka waktu yang sudah ditentukan peneliti melakukan pengamatan terhadap fenomena yang terjadi (W.Lawrence Newman:2007,18)

3.4 Teknik Pengumpulan Data

3.4.1 Wawancara

Wawancara adalh suatu kegiatan yang dilakukan untuk mendapatkan informasi secara langsung dengan mengungkapkan pertanyaan-pertanyaan pada responden Peneliti akan menggunakan teknik pengumpulan data (Subagyo,Joko,2004:39) wawancara dilakukan dengan cara mewawancarai para informan dalam jangka waktu 2 bulan selama peneliti melakukan penelitian. Wawancara dilakukan untuk mendapat berbagai informasi menyangkut masalah yang diajukan dalam penelitian wawancara akan dilakukan kepada informan yang memiliki kapasitas dalam memberikan informasi mengenai data center.

Dalam memperoleh informan dengan cara menggunakan teknik *snow ball* dimana pada informan pertama memberikan rujukan kepada informan selanjutnya yang dirasa memahami permasalahan penelitian. Dalam pengumpulan data, peneliti memiliki *gate keeper* yang fungsinya menghubungkan peneliti dengan sumber data. Gate keeper mengarahkan dan memberikan rujukan informan lainya yang dirasa memiliki kepentingan dalam menentukan dan memahami proses analisa risiko. Pada penelitian ini Gate keeper (IP) sebagai

informan pertama. Gate keeper menjabat sebagai staf divisi facility yang bertugas untuk menjaga peralatan dan akses masuk kedalam ruang data center. Setelah melalui proses wawancara dengan informan pertama yang sekaligus juga sebagai gate keeper, peneliti melanjutkan wawancara sesuai dengan rujukan dari informan pertama. Peneliti melanjutkan wawancara kepada staff keamanan (AG) Informan yang memiliki kapasitas dalam memberikan keterangan lain personel sekuriti yang berjaga di lantai dimana data center berlokasi. Peneliti akan mewawancarai bagaimana proses para personil sekuriti memastikan keamanan data center dan hambatan-hambatan baik ancaman maupun kerentanan yang dialami selama mengamankan data center. Setelahnya peneliti juga mewawancarai (AS) selaku manajer assurance yang berkapasits membuat flowchart,dan standarisasi mutu yang dibutuhkan untuk sertifikasi. Peneliti juga mewawancarai SD selaku pelanggan data center, namu ketika mewwancarai SD beliau tidak berkenan untuk direkam, wawancara dilakukan sebatas mendapatkan gambaran mengenai alasan customer melakukan *colocation* di data center milik PT ”X” Untuk memudahkan dalam melakukan pengolahan data lapangan, peneliti dengan menggunakan handphone melakukan record terhadap informan. Hasil rekaman kemudian dipisahkan berdasarkan informasi yang dibutuhkan. Hasil wawancara yang menunjang data penelitian akan dicantumkan dalam lampiran verbatim. Setelah melakukan *record* peneliti menganalisis informasi tersebut sehingga menjadi sumber data lapangan.

3.4.2 Observasi

Nasution (1998) menyatakan bahwa, observasi adalah dasar semua ilmu pengetahuan. Para ilmuwan hanya dapat bekerja berdasarkan data yaitu fakta mengenai dunia kenyataan yang diperoleh melalui observasi. Sanafiah Faisal (1990) mengklasifikasikan observasi menjadi observasi Berpartisipasi (*participant observation*), observasi yang secara terang-terangan dan tersamar (*overt observation dan covert observation*), dan observasi yang tak berstruktur (*unstructured observation*) (Sugiyono, 2005: 64-66) Penelitian ini berjenis penelitian kualitatif, sehingga pengumpulan data dilakukan dengan menggunakan metode penelitian lapangan, karena peneliti akan turun langsung ke lokasi data

center yang menjadi lokasi penelitian untuk diobservasi dan berinteraksi langsung dengan informan yang dapat memberikan informasi kepada peneliti. Peneliti akan melihat langsung bagaimana proses pengamanan data center yang sedang dijalankan, bagaimana alur pengambilan keputusan, dan proses evaluasi dari kegiatan pengamanan yang telah dilakukan. Observasi dilakukan pada aktifitas melihat risiko pencurian data yang terdapat pada lokasi data center. Observasi dilaksanakan untuk melihat antara lain :

- Melihat bentuk pengamanan yang dilakukan pihak managemen gedung dalam memberikan akses masuk kepada pengunjung termasuk penerapan SOP keamanan

- Melihat aktifitas penerapan ID card sebagai akses masuk kedalam lokasi data center, saat ditempelkan kedalam ke mesin.

- Melakukan percobaan terhadap ID card departemen lain yang tidak berwenang masuk kedalam lokasi data center, apakah ID card tersebut memiliki akses masuk atau tidak.

- Melihat sitem pengamanan lainya dalam mengurangi risiko pencurian data. Dalam hal ini peneliti melihat bentuk keamanan-keamanan lain seperti peletakan CCTV, bentuk desain ruangan, tempat pengawasan, dan pengamanan ruang koleksi.

- Melihat bentuk pengawasan dan keamanan pada setiap rak data center. Melihat cara kerja petugas dalam melakukan pelayanan dan pengawasan terhadap pelanggan data center yang dating untuk melakukan pengecekan terhadap kondisi *server*

- Melihat penerapan SOP pemberian akses masuk ke ruangan data center

Observasi dilakukan secara terbuka dimana keberadaan penulis diketahui oleh subyek penelitian. Penulis dalam observasi ini dapat melihat secara langsung

pelaksanaan aktifitas pengamanan dan operasional data center. Dalam observasi ini penulis juga menanyakan beberapa hal dengan petugas lapangan namun tidak direkam melainkan menggunakan catatan lapangan (field notes) Dari pertanyaan-pertanyaan yang diajukan oleh peneliti maka informasi yang didapatkan dirasakan cukup. Karena data center merupakan salah satu bisnis perusahaan yang sangat krusial karena berkaitan dengan data pelanggan yang mungkin sangat penting, maka peneliti memerlukan waktu yang cukup lama untuk membangun rapor dengan para informan. Namun Observasi baru dilakukan mulai tanggal 9 Januari – 26 Mei 2012

3.4.3 Studi Literatur dan Kepustakaan

Dimaksudkan untuk memperoleh bahan-bahan tertulis yang berkaitan dengan permasalahan yang dikaji, yang akan membantu dalam memberikan pemahaman akan penelitian social ini. Serta untuk melengkapi data primer yang diperoleh oleh penulis di lapangan. Hal yang dilakukan dalam studi kepustakaan ini adalah mempelajari bahan-bahan kepustakaan yang ada hubungannya dengan permasalahan analisa risiko, dan pengamanan data. Selain itu Studi kepustakaan dalam penelitian ini, bertujuan untuk merumuskan latar belakang masalah, permasalahan, kerangka pemikiran dan kerangka konseptual yang digunakan sebagai landasan dasar penelitian

3.5 Teknik Analisa Data

Dalam penelitian kualitatif, analisa data dalam praktejnya tidak dapat dipisahkan dengan proses pengumpulan data. Kedua kegiatan ini harus dilakukan dengan serempak, artinya analisa data dikerjakan bersama dengan pengumpulan data, dan dilanjutkan setelah pengumpulan data selesai. Dengan demikian secara teoritik analisa dan pengumpulan data dilaksanakan secara berulang yang ditujukan agar masalah dapat terpecahkan.

S.Nasution mengemukakan bahwa analisis data kualitatif adalah penyusunan data (menggolongkannya dalam tema dan kategori) (Nasution,) Hal ini sejalan dengan moleonng yang mengatakan bahwa analisis data dalam penelitiah kualitatif adalah

proses mengatur urutan data,mengorganisasikannya ke dalam suatu pola, kategori dan situasi uraian dasar. Dengan demikian dalam analisa data kualitatif diperlukan data kreatif dari peneliti untuk mengelolanya sehingga bermakna. (Moleong)

Untuk melakukan analisa data guna memperoleh data yang valid dan meyakinkan, maka peneliti harus melakukan pengorganisasian data, pengelompokan data, dan mengurutkan data yang diperoleh dari hasi observasi,wawancara dan dokumentasi.

BAB IV

GAMBARAN UMUM DATA CENTER PT "X"

4.1 Sejarah Didirikannya Data center PT "X"

Data center PT "X" didirikan oleh PT "X" pada tahun 2005. sebagai perusahaan yang bergerak di bidang telekomunikasi PT "X" memperluas bidang usahanya dengan menyediakan penyewaan rack untuk *colocation* server. PT "X" berlokasi di 3 lantai dalam sebuah gedung perkatoran di daerah jakarta pusat. PT "X" menggunakan lantai 2,6 dan9, sedangkan data center berlokasi di lantai 6. Awal didirikannya data center PT "X" hanya memiliki 2 ruangan, dengan jumlah rack hanya sebanyak 30 buah dengan kapasitas 42 U. Dengan tingginya peminat data center maka PT "X" menambah luas ruangan data center dan membeli rack baru, sehingga sekarang data center PT "X" dibagi menjadi 3 ruangan dengan jumlah rack sebanyak 68 dengan jumlah server sebanyak 10 rack untuk kepeluan internal PT "X". Data center PT "X" menjual layanan, *Collocation. Collocation* merupakan layanan penyewaan space untuk server, para pelanggan dapat menyimpan server nya di rack milik PT "X", rack yang disewakan oleh PT "X" paling kecil dengan kapasitas 14 U dengan harga 3juta perbulan, 21 U dengan harga 7 juta perbulan dan 11 juta untuk kapasitas 42 U. Dengan melakukan *colocation*, pelanggan tidak perlu memikirkan lagi bagaimana perawatan dan menjaga lokasi server mereka. PT "X" bertanggung jawab untuk menyediakan keamanan, dan lingkungan yang mendukung server mereka agar dapat beroprasi dengan baik. Pelayanan yang PT "X" berikan adalah, menyediakan listrik untuk server, ruangan dengan kelembabab dan suhu yang selalu dipantau dan keamanan selama 24 jam dalam satu hari.

4.2 Ruangan Data Center PT "X"

4.2.1 Data center 1

53

Ruangan I ini luasnya 10 x 8 m^2 dengan jumlah rak sebanyak 30 rak, 30 rak ini terdiri dari server dengan kapasitas 14 u,21 u dan 42 u. Dari sebanyak 30 rak yang ada, 10 rak diantaranya digunakan untuk kebutuhan data center internal.

Ruangan ini diawasi dengan 4 buah CCTV yang diletakkan disetiap *row* (baris) server. Dalam ruangan ini terdapat 30 *customer* yang melakukan *collocation* di server yang disewakan oleh PT "X" dari 30 orang *customer* tersebut ada 1 perusahaan yang membawa sendiri servernya.

4.2.2 Data Center 2

Ruangan ini tidak disewakan karena diisi oleh *server* dari berbagai perusahaan, ruangan dimana banyak perusahaan penyedia jasa telekomunikasi yang mengalokasikan servernya agar dapat saling terhubung satu sama lain.

4.2.3 Data Center 3

Dari ketiga ruangan, ruangan ketiga ini merupakan ruangan terluas di area data center. Ruangan ini berluas 700 m^2, terdiri dari 8 row (baris) yang memuat 48 *rack*. Ruangan ini di awasi oleh 6 CCTV, yang diletakan di koridor 2 dan 5, di area *secure cage* 2 dan 3 serta di depan UPS. Di ruangan ini terdapat sekitar 52 customer yang melakukan colocation server di data center PT 'X" namun dari 48 *rack* yang ada di ruangan ini,3 diantaranya merupakan server yang dibawa sendiri oleh customer, PT "X" hanya menyediakan tempat (space)

4.3 Fasilitas Data center

Karena Data center merupakan rumah dari sumber daya komputasi yang sifatnya kritis, perusahaan penyedia layanan harus membuat perjanjian khusus dengan fasilitas dan personil yang dibutuhkan untuk beropreasi 24 jam selama

seminggu. Fasilitas ini harus mendukung seluruh sumber daya server dan infrastruktur jaringan. Tuntutan yang kekritisan bisnis dari setiap aplikasi yang ada di data center, membuat kebutuhan untuk dapat mengatatasi bidang-bidang berikut:

4.3.1 Kapasitas daya

Kapasitas daya pada Data center PT “X’ bersumber dari PLN setempat, jika terjadi pemadaman listik. Data center di support oleh 2 UPS dengan kapasitas 2 x160 KVA. UPS ini mampu memndukung daya yang dibutuhkan oleh data center selama 3 jam sebelum listrik dari PLN kembali menyala.

4.3.2 Kapasitas pendingin

Data center pada PT "X" didukung oleh AC dengan kapasitas yang berjumlah 6 buah, yang dapat mendinginkan sampai batas terendah +- 16 derajat celcius.

4.3.3 Pengawasan terhadap suhu dan kelembaban

Pengawasan suhu dilakukan secara berkala oleh tim facility PT ”X” dengan mengecek suhu ruangan menggunakan alat pengawas suhu.

4.3.4 Sistem pengawas api dan asap

Data center PT ‘X’ menggunakan FM 200 sebagai pemadam kebakaran, jika alarm kebakaran berbunyi maka FM 200 akan mengeluarkangas FM 200 yang akan mematikan api, dengan menghisap semua gas oksigen yang ada diruangan tersebut.

4.3.5 Keamanan fisik: membatasi akses dan sistem pengawasan

Pengamanan pada ruangan data center PT "X" dilakukan dengan menempatkan petugas keamanan di pintu masuk data center serta menggunakan *CCTV* dan pintu dengan *ID card*

4.4 Kejahatan dan Potensi Pencurian Data Pada Ruang *Data Center*

Untuk data pencurian yang pernah terjadi di Data center, pihak Keamanan data center mengatakaan tidak memiliki data mengenai tindak pencurian data yang pernah terjadi disana. Untuk memperoleh data pencurian server, peneliti telah berulang kali menanyakan tentang data pncurian, tetapi hampir seluruh petugas mengatakan tidak terdapat data pencurian. Mungkin data tersebut memang tidak ada atau data tersebut tidak dapat dipublikasikan demi kepentikan reputasi petugas keamanan dan untuk menjaga kredibilitas jasa layanan penyewaan Server pada perusahaan tersebut.Sehingga data yang diperoleh merupakan data hasil wawancara dengan informan.

Hasil wawancara dengan informan mengatakan bahwa Tidak pernah ada pencurian yang terjadi, pelanggaran yang terjadi atas ruang data center hanya seputar pelanggaran prosedur pemberian akses masuk ke ruang data center. Selama ini banyak pengunjung yang masuk ke ruangan data center tidak menunjukkan berkas-berkas yang dibutuhkan, seperti form auotorisasi (terlampir). Banyak dari pengunjung data center yang dating karena sudah sering datang ke ruangan data center, dan mengenal baik petugas keamanan sehingga tidak lagi menunjukkan form tersebut. Yang menjadi kendala pihak keamanan dalam menjalankan tugasnya karena, pihak keamanan data center tidak berdiri sendiri, mereka juga harus mengamankan aset perusahaan lainnya, karena hanya ada 1 pos keamanan di PT "X" yaitu di lantai 6, dimana data center berlokasi.

4.5 Kemanan yang ada di Ruangan Data Center

Perusahaan X, dalam mengurangi risiko pencurian data di ruangan servernya menggunakan keamanan fisik maupun elektronik. Keamanan fisik dan elektronik tersebut meliputi :

4.5.1 *CCTV (Closed Circuit Televition)*

CCTV merupakan kamera pengawas yang dapat merekam peristiwa kejadian dalam rentan waktu tertentu. Untuk Ruangan Server, pemasangan CCTV terdapat pada setiap koridor pada ruang server, pintu masuk, keluar masuk lift dan tangga darurat dan di dalam ruang perkantoran staff dan petugas. CCTV ini

bekerja 24 jam. CCTV di data center PT ‘X’ menggunakan teknologi yang dapat langsung merekam setiap hal yang ditangkap oleh CCTV. Pusat monitor pengawasan CCTV berada di ruang sekuriti yang seluruhnya terdapat dilantai 6.

4.5.2 Pintu dengan menggunakan ID Card

Pintu dengan menggunakan ID card terdapat pada seluruh akses masuk ke ruangan data center. Pintu ini hanya terbuka apabila terhubung dengan kartu ID dengan menekan nomor pin yang telah terautorisasi. Tidak semua ID card dan PIN dapat mengakses ruangan ini, hanya PIN dari orang-orang dalam beberapa departemen yang berkepentingan masuk yang bisa mengakses ruangan data center. Beberapa divisi yang berkepentingan masuk antara lain:

- Facility Engineering, divisi ini memiliki tugsa untuk memaintain semua fasilitas didalam PT ‘X’ termasuk semua fasilitas yang ad adi ruangan data center, meliputin AC,pemadam kebakaran,UPS dll. Anggota Facility divisi saat berjumlah 10 orang yang bertugas tidak hanya untuk memantau ruang data center tetapi juga seluruh fasilitas di PT “X”
- TAC, Technical Assistace Center, divisi ini bertugas untuk memaintain fasilitas CCTV diseluruh ruangan yang ada di PT “X” termasuk ruangan data center.
- *Account Executive* Data Center, Para sales data center memiliki autorisasi untuk memasuki ruang data center dengan kepentingan mendampingi setiap pelanggan yang datang. Saat ini jumlah sales data center berjumlah 5 orang dengan status pegawai tetap.
- Office Boy, Ada beberapa office boy yang diberikan akses masuk kedalam ruang server dengan kepentingan untuk membersihkan area data center.

4.6 Jumlah petugas keamanan yang ada pada Data center

Pada Ruang data center terdapat petugas keamanan yang berjaga didepan pintu masuk data center yang tugasnya mengecek semua berkas yang dibutuhkan seperti melakukan pengecekan atas form autorisasi dengan pengunjung yang dating, memberikan kunci rak,mengembalikan kunci rak. untuk memasuki ruangan data center. Petugas keamanan data center berjumlah 5 orang, dengan pembagian tugas sebagai berikut:

Hari kerja : 2 orang jaga pagi, 2 orang jaga malam

Hari Libur :1 orang jaga pagi, 2 orang jaga malam.

Untuk semua petugas keamanan yang menjaga ruangan keamanan merupakan tenaga kerja yang didapat dari pihak ketiga (outsourcing)

4.7 Jumlah Petugas yang Melakukan Pelayanan dan Pengawasan Pada Ruangan Server

Untuk melakukan pelayanan terhadap pengunjung data center, PT "X" masih menggunakan tenaga yang sama dengan petugas keamanan untuk pengamanan kantor operasional PT "X". Namun selain dari petugas PT "X' ada juga customer yang membawa sendiri personel keamanannya. Customer tersebut merupakan salah satu Bank asing yang mengalokasikan servernya di PT 'X' untuk melakukan pengamanan Bank asing tersebut menggunakan pihak ketiga, yaitu perusahaan sekuriti yang cukup ternama.

4.8 Persyaratan mengunjungi data center

4.8.1 Terdaftar dalam *form autorhized*

Setelah menyewa server pada data center PT 'X'. Customer akan diberikan form autorisasi, dalam form autorisasi terdaftar beberapa nama yang diberikan kuasa untuk menjadi penanggung jawab dari customer tersebut. persyaratan yang harus dipenuhi antara lain, surat kuasa dan KTP. setelah terdaftar dalam form autorisasi, maka setiap orang yang terdaftar akan diberikan user name dan password untuk dapat log in ke buku tamu data center yang harus diisi setiap kali

berkunjung ke data center. untuk pengunjung internal, yang memiliki akses untuk masuk adalah divisi facility, tac, sales data center dan seluruh manager di PT 'X'. namun jika ada keperluan internal selain dari divisi tersebut dapat diberikan hak autorisasi dengan mengisi form internal yang ada di intranet perusahaan. setelah menjelaskan keperluan dan di setuji oleh manager facility maka pihak dari divisi facility akan mendampingi untuk masuk kedalam data center.

4.8.2 Melapor pada sekuriti

Ketika datang untuk mengunjungi data center, pengunjung harus melapor terlebih dahulu kepada petugas keamanan. untuk mengisi buku tamu yang berisi jam masuk, jam keluar dan keperluan memasuki data center. Setelah melapor pengunjung akan diberikan ID card dan nomer PIN khusus pengunjung.

4.8.3 Mengisi log in buku tamu elektronik

Setelah melapor ke pihak keamanan, pengunjung harus mengisi log in buku tamu elektronik, untuk log in kedalam sistem ini pengunjung harus menggunakan user name dan password yang diberikan ketika namanya sudah terdaftar di form autorized. Log in ini dimaksudkan akan semua berkas dan data pengunjung yang datang dapat terintegrasi dalam sistem. selain itu daftar ini juga dimaksudkan agar dapat mengecek jika ada kerusakan atau kehilangan dengan melihat siapa yang terakhir log in. daftar ini berisi tabel nama perusahaan, jam masuk, lokasi server, keperluan dan jam keluar. dalam tabel ini dibagi kedalam 3 warna, yaitu putih,kuning,dan merah. Putih berarti pengunjung masih berada didalam server, kuning sudah selesai melakukan kunjungan dan merah jika kunjungan dibatalkan.

4.9 Asset yang terdapat dalam ruang data center

Data center memiliki komponen yang menunjang infrastruktur kebutuhan Informasi teknologi yang berfungsi untuk pertukaran data. Dan berikut ini adalah asset yang dimiliki oleh PT “X” yang dikelola oleh facility division :

4.9.1 Rack

Rack system adalah rack yang khusus di rancang untuk penempatan server ataupun peralatan jaringan network seperti switch dan komputer server .Manfaat rack adalah lebih kepada efisiensi ruang atau tempat, juga komputer maupunperalatan akan lebih mudah dalam maintenancenya.

PT "X" memiliki 68 rack dari berbagai merek dengan kapasitas 42 U. Diantaranya:

- o 18 rack fortuna
- o 18 rack fujitsu
- o 12 rack HP *(hewlett packard)*
- o 20 rack IBM

Rack-rack tersebut disewakan dengan harga 11.000.000 untuk setiap 42 U, berarti setiap bulan biaya sewa yang didapat oleh PT "X" sebanyak: 82 x11.000.000= 902.000.000 rupiah setiap bulannya. Dengan nilai kontrak 902.000.000 x 12 bulan = 10.824.000.000 dalam setahun

4.9.2 Server

Terdapat banyak aplikasi yang juga dicollocation di server milik PT "X" dan jaringan infrastruktur seperti server proxy dhcp dan lainnya. Sehingga membutuhkan berbagai macam server untuk pengoprasiannya. Server tersebut terdiri dari:

- o operating sistem : windows sever 2003 dan red heat 5.0
- o hardware : IBM blade server, HP server, Dell, fujitsu dan SUN sever

4.9.3 AC

AC (Air Conditioner) pada ruang data center berfungsi sebagai pendingin ruangan agar server yang terdapat di dalamnya dapat terjaga suhunya yang berkisar antara 16 derajat-21 derajat celcius. Suhu ini merupakan batas normal

untuk ruangan data center, jika terlalu rendah maka akan menimbulkan embun yang dapat merusak komponen server, jika terlalu tinggi dapat mengakibatkan korsletnya kabel. PT "X" menggunakan AC khusus data center dengan merk Libert, AC Libert yang PT "X" miliki sebanyak 4 unit, dengan alokasi Data center 1 1 unit, Data center 2 1 unit, dan Data center 3 2 unit.

4.9.4 Switch

Switch digunakan sebagai distribusi jaringan. Swicth adalah sebuah alat jaringan yang melakukan bridging transparan (penghubung segementasi banyak jaringan dengan *forwarding* berdasarkan alamat MAC) Switch jaringan dapat digunakan sebagai penghubung komputer atau router pada satu area yang terbatas, switch juga bekerja pada lapisan data link, cara kerja switch hampir sama seperti bridge, tetapi switch memiliki sejumlah port sehingga sering dinamakan *multi-port* bridge. (www.apteknologi.com) Switch yang ada di data center PT "X" menggunakan berbagai merk dari beberapa vendor terkemuka diantaranya :

- Cisco : catalys 4503, 3750G
- Linksys : SWR224
- Allied Telesyn : AT-8024GB

4.9.5 Router dan Firewall

Router digunakan sebagai alat penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Dan *firewall* memiliki Fungsi mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi oleh *firewall. Firewal*l melakukannya dengan melakukan inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, kemudian melakukan penapisan (filtering) terhadap koneksi berdasarkan hasil inspeksi paket dan koneksi tersebut. Router

yang digunakan oleh PT "X" adalah cisco seri 2800 Firewall yang di gunakan adalah cisco ASA 5540

4.9.6 Wireless LAN dan Pengatur bandwidth

Wireless Local area Network (WLAN) tersebar dibeberapa titik di seluruh area kantor PT "X". WLAN memiliki controller yang berguna untuk distribusi IP. Perangkat ini terdapat pada data center bermerek cisco 4400 series. Pengatur bandwitdh berguna sekali untuk kecepatan distribusi data dan alur kecepatan konektifitas intranet. PT "X" menggunakan alat bernama allot net enforcer tipe AC-1400

4.9.6 UPS

Uninterruptible power supply (disingkat UPS) adalah perangkat yang biasanya menggunakan baterai backup sebagai catuan daya alternatif, untuk Dapat memberikan suplai daya yang tidak terganggu untuk perangkat elektronik yang terpasang. UPS yang digunakan adalah merk APC dan MGE. PT "X" menggunakan 2 UPS dengan kapasitas 2 x 160 KVA/ 2 x 128 KW

4.9.7 Perangkat Pendukung Lain

Selain perangkat utama yang telah disebutkan diatas PT "X" juga memiliki pelengkap lain seperti perangkat;

1. Mailgate Axway

   Perangkat ini berfungsi sebagai spam assassin dan juga berfungsi sebagai proteksi mail dari virus.

2. File Transfer Direct Axway

   Alat ini berfungsi sebagai pemindah file yang dapat memuat lampiran data hingga 2 Gigabyte.

3. WCS Cisco

Merupakan perangkat dari cisco yang berfungsi untuk mengatur akses, authentifikasi dan authorisasi dari pengguna wireless yang tersebar di PT "X"

4.10 Kategori Data Center PT "X"

Jika di tinjau dari tingkatan tier pada perancangan data center menurut TIA (*Telecommunication Industry Association)*

4.11 Kerentanan dan Ancaman Pusat Data PT "X"

Sebelumnya resiko merupakan persingungan antara asset,kerentanan dan ancaman. Pusat data sangat rentan pada ancaman yang dapat mempengaruhi seluruh jaringan perusahaan dan terhadap ancaman yang spesifik di pusat data berikut ini merupakan ancaman yang umumnya timbul pada pusat data (Arregoces et all: 2004,160)

• *DoS (Denial Of Service)*

Tujuan dari ancaman *DoS* adalah menurunkan layanan hingga pemilik sah dari server tersebut tidak dapat lagi melakukan kegiatan ruting mereka,seperti pemeliharaan,pemantauan dan sebagainya. Ancaman *DoS* dapat dilakukan dengan berbagai cara, namun kasus yang paling umum *DoS* dirancang untuk menghasilkan volume data yang besar sehingga mengkonsumsi sumber daya yang jumlahnya terbatas seperti bandwidth, siklus *CPU*, dan menghalangi pemilik server untuk masuk ke dalam memori servernya.

- Pelanggaran Informasi rahasia
- Pencurian Identitas
- Pencurian atau perubahan data
- Penggunaan komputer dengan akses yang tidak sah
- Akses yang tidak dibenarkan

Terdiri dari melakukan akses ke sumber data dengan menggunakan akun yang valid milik orang lain atau yang dikenal dengan istilah *"backdoor"* yaitu

setiap metode tersembunyi untuk memperoleh akses remote ke komputer atau sistem lainnya. Penyusupan akun merupakan peristiwa pelanggaran keamanan yang serius yang dapat mengakibatkan hilangnya data, pengubahan data, dan bahkan pencurian layanan. Dalam konteks Pusat Data, ancaman serangan akses tidak sah sering terjadi pada web server dengan kontrol otentikasi yang minim.

Selain ancaman, pusat data juga memiliki kerentanan yang dapat menimbulkan resiko terjadinya pencurian data. Kerentanan yang terdapat pada pusat data terdapat pada area berikut ini (Arregoces et all: 2004,161) :

- Implementasi perangkat

  Software dan kelemahan protokol,desain software yang salah,pengujian tidak lengkap, dll

- Konfigurasi

  Unsur yang tidak dikonfigurasi dengan benar,lalainya penggunaan standar, dan sebagainya.

- Desain

  Desain tidak efektif atau tidak memadai untuk menjalankan sistem keamanan, kurangnya atau pelaksanaan mekanisme redundansi yang tidak tepat , dll. Pada PT "X" desain gedung yang tidak ditujukan sebagai data center, mengakibatkan tidak fokusnya pengamanan yang dilakukan, hal ini dibuktikan dengan tugas yang diberikan kepada personel keamanan tidak hanya mengamankan data center namun juga untuk mengamankan aset

- Personel keamanan

  Personel keamanan yang dimiliki oleh PT "X" dalam mengamankan data center merupakan personel keamanan yang didapat dari pihak ketiga *(outsource)* hal ini tentu saja sangat berisiko karena personel keamanan dapat saja membocorkan metode keamanan pada orang luar. Selain itu

personel keamanan yang dipekerjakan tidak didapat berdasarkan kualifikasi khusus, namun hanya kualifikasi lulus SMA tidak ada persyaratan, seperti mampu menganalisa sebuah kasus dan kemampuan lainnya.

Gambar 3.1

Gambar Klasifikasi Data Center

	Tier 1 Basic Site Infrastructure	Tier 2 Redundant Capacity Components	Tier 3 Concurrently Maintainable	Tier 4 Fault Tolerant
Building Type	Tenant	Tenant	Stand-alone	Stand-alone
Staffing	None	1 Shift	1+ Shifts	24 by Forever
Representative Site Availability	99.67%	99.75%	99.98%	99.99%
Typical kW per Cabinet	<1kW	1-2 kW	>3 kW	>4 kW
UPS Redundancy	N	N+1	N+1	2N
Generator	No generator, or optional	Generator	N+1 Generator	2N Generator System
Interface with Building Management System	No	No	Yes	Yes

(Sumber :Arregoces,Mauricio:2004,297)

Datacenter PT "X" berada pada tingkatan *TIER II-Redundant Components*

"iya ini tier 2 kan kita udah ada redundant, maksudnya itu kita ada back up nya, kalo kita mati kan kita ada back up dr cabang, kalo listrik kita ada UPS yang bisa nahan 3 jam sebelum listrik PLN nyala, lantai kita juga raised floor dan data center kita kan ditujukan buat keperluan perusahaan,soalnya kan ini gedung kita jadi tenat, gak berdiri sendiri buat data center,data center yang baik mah gak digedung perkatoran. Nah kalo data center tier 4, dia

harus punya back up power pesaing PLN, yang sebesar itu dayanya di Indonesia belum ada tier 4" (I.P,15 Februari)

BAB V

ANALISA DATA

5.1 Praktek Analisa Risiko Kualitatif PT "X"

Risiko merupakan unsur ketidakpastian dalam suatu usaha,kemungkinan bahwa keuntungan yang diharapkan dimasa mendatang akan menyimpang dari target yang telah ditentukan. Risiko didefinisikan sebagai kemungkinan terjadinya eksploitasi terhadap kerentanan oleh ancaman dari luar sehingga menyebabkan kerugian kepada aset. Karena data center menyimpan data pelanggan yang sangat penting bagi keberlansungan usaha mereka, maka perlu dilakukan analisa risiko yang dapat digunakan sebagai bahan pertimbangan untuk melakukan *project management* bagi keamanan data center. Dalam buku *Project management* disebutkan bahwa untuk melakukan analisa risiko diperlukan input yang berasal dari beberapa proses sebelumnya, seperti *risk management plan, risk register, project scope statement dan organizional procces asset*. Setelah mengumpulkan semua input , maka data-data tersebut diolah dengan menggunakan beberapa teknik analisa yang dapat dipilih yaitu *risk and impact assessment, risk and impact matrix, expert analysis,* dan analisa tersebut akan menghasilkan risk register yang diupdate yang dapat digunakan sebagai bahan pertimbangan untuk melakukan analisa risiko selanjutnya dikemudian hari. Analisa risiko kualitatif akan menjadi dasar untuk melakukan analisa kuantitatif dikemudian hari. Karena banyaknya keterbatasan PT "X" maka PT "X" dalam hal menganalisaa risiko menggunakan teknik analisa risiko kualitatif, dikarenakan;

- Tidak adanya tenaga ahli, seperti risiko analis yang dapat melakukan analisa risiko kuantitatif yang bersifat lebih kompleks
- Tidak lengkapnya data historis mengenai kejahatan yang pernah terjadi di data center.

- Belum mapannya proses penanganan risiko yang dibuktikan tidak adanya divisi khusus yang didelegasikan untuk menangani risiko yang dihadapi oleh PT “X.

5.1.1 Mengumpulkan input

Sebelum melakukan analisa risiko, analis memerlukan beberapa input sebagai bahan analisa yang terdiri beberapa dokumen;

5.1.1.1 Risk Register

5.1.1.1.1 *Risk Register Input*

5.1.1.1.1.1 *Risk Management Plan*

Dari beberapa pilihan strategi yang dapat dilakukan untuk memanajemenkan risiko PT "X" memilih untuk mengurangi risiko dengan menggunakan teknologi yang dapat mendukung perusahaan untuk melakukan operasional Data center PT “X”. Untuk Rencana Manajemen Risiko yang yang dibuat tidak ada dokumen dengan standar tertentu seperti rencana manajemen risiko yang seharusnya memuat, bagaimana, berapa biaya yang dibutuhkan, dan jangka waktu yang ditetapkan untuk melakukan manajemen risiko.

> “kita sih kalo untuk risiko kita lebih prefer buat mengurangi ya, karena kalo dihilangkan nggak bisa dan kita juga gak mindahin risiko ke pihak ketiga atau asuransi, itu kan emang perusahaannya yang masukin asuransi sendiri kalo emang mau colo disini, kalo untuk ,mengurangi risiko kita menggunakan alat-alat yang canggih, untuk alat-alat itu kan kita bayar ya biaya manajemen risiko nya masuk kesitu lah” (A.S 18 November 2012)

Manajemen risiko yang dilakukan oleh PT "X" hanya berupa tindakan yang dilakukan untuk mengurangi kemungkinan pencurian. Selain dengan menggunakan peralatan yang sudah ada, PT “X” juga mengurangi risiko kehilangan data dengan melakukan kontrol setiap hari terhadap fisik data center, control tersebut dilakukan oleh pihak facility. PT “X” belum memiliki asuransi

untuk keamanan server, asuransi dibebankan kepada pelanggan yang melakukan *colocation* server di rack milik PT “X”

5.1.1.1.1.2 *Activity Cost Estimates*

Biaya untuk melakukan aktifitas identifikasi risiko yang ada di PT “X” belum dibuat secara khusus yang ditujukan untuk membuat identifikasi risiko, biaya yang ada masih disatukan dengan biaya operasional sehari-hari yang dilakukan oleh pihak facility yang bersinggungan langsung dengan operasional pemeliharaan data center. Belum adanya perhitungan yang baik mengenai biaya yang akan ditimbulkan oleh risiko, perhitungan biaya yang akan ditimbulkan masih bersifat estimasi. hal ini dibuktikan ketika peneliti menanyakan hal ini kepada manager assurance yang berkapasitas dalam menangani SOP yang ada di PT "X"

> "Disini belum dihitung mengenai biaya identifikasi risiko, itu aja gak ada gimana mau tau biaya dari risiko yang ditimbulkan, baru mau dibuat skemanya,ini gw baru mau bikin aset skemanya, baru mau gw data'in, belom gw share ke manajer-manajernya. Aturan sih ntar setiap manajer ntar isi aset di departemen mereka apa aja . Itu emang kudu dibuat sih,soalnya abis audit sertifikasi ISO kemarinkan itu emang salah satu temuannya, tapi pasti nanti dibuat sih, masih dalam proses lah” (AS 18 November 2012)

5.1.1.1.3 Estimasi Jangka Waktu Kegiatan Identifikasi Risiko

Karena belum adanya pelaksanaan identifikasi risiko yang dilakukan dengan persiapan yang baik, PT “X” juga belum memiliki estimasi jangka waktu untuk melakukan kegiatan identifikasi risiko.seluruh kegiatan yang selama ini berlangsung merupakan kegiatan rutin yang akan terus dilakukan oleh pihak facility dan keamanan sampai ada keputusan dari manajemen untuk menghentikan kegiatan tersebut.

5.1.1.1.4 *Stakeholder Register*

Selain deskripsi mengenai faktor-faktor yang mempengaruhi perusahaan, dalam membuat risk register juga diperlukan stakeholder register yang berisi deksripsi hal yang dibutuhkan oleh s*takeholder*, jika dilihat dari deskripsi mengenai stakeholder register, maka stakeholder dapat dibagi kedalam dua bagian, stake holder internal dalam hal ini para karyawan yang bersinggungan langsung dengan operasional data center seperti sales marketing tim, faciliti divisi, dan sebagainya. Stakeholder eksternal yaitu para pelanggan dan para vendor,dalam hal ini penyedia peralatan kebutuhan data center. Stakeholder register ini belum dibuat dengan baik,hanya ada dokumen kontrak dengan pelanggan yang jelas mencakup hak dan kewajiban para pelanggan.

> "Stakeholder?kita sih belum punya yang secara jelas, apalagi ngebagi internal eksternal palingan kalo buat pelanggan kita pake SLA, service level agreement,pelanggan juga stakeholder kita kan? Secara dia yang make jasa kita, nah kita berpedoman berdasarkan itu aja tuh" (AS 18 November 2012)

5.1.1.1.5 Rencana Pengelolaan Biaya

Pengelooan biaya identifikasi risiko belum dibuat dikarenakan belum adanya alokasi dana yang secara khusus ditujukan untuk melakukan identifikasi risiko. Pengelolaan biaya maintenance yang selama ini dijalankan itu diasumsikan oleh para staf facility PT "X" sebagai biaya untuk pencegahan risiko yang akan muncul. Selain belum ada alokasi dana, anggota tim facility juga tidak mengerti apa yang dimaksud dengan rencana pengelolaan biaya risiko yang diidentifikasi, hal ini dapat dilihat dari belum dapatnya para anggota tim untuk membedakan biaya identifikasi risiko dengan biaya pelaksanaan operasional data center. Seperti yang dikatakan IP slah satu informan yang bersikeras telah melakukan pengelolaan biaya karena sudah mengeluarkan anggaran untuk melakukan perawatan yang sudah tentu berbeda dengan pengelolaan biaya identifikasi risiko yang dimaksud

> "biaya manajemen risiko? Gak ada itu sih, kita biaya pasti lah ada alokasi buat divisi facility, tapi itu buat biaya maintenance, itu buat preventif lah ya,

kita jaga AC, kita jaga CCTV supaya data center kita gak rusak kalo AC nya gak mati, supaya kita tetep bisa ngawasin pake CCTV, alokasi budget tahunan sih buat itu, selain buat maintenance ya juga buat beli-beli barang, kan tugas facility juga beli-beli barang peralatan, kita cari vendor ntar bikin PR , PO baru bayar. Kalo biaya sih paling yang kita keluarin buat itu aja" (15 Februari 2012)

5.1.1.1.6 Perencanaan Pengelolaan Jadwal

Dalam melakukan identifikasi risiko, PT "X" belum memiliki estimasi jangka waktu yang akan ditempuh untuk melakukan identifikasi risiko sebagai bahan untuk membuat risk register (daftar risiko) hal ini menyebabkan PT "X" juga belum memiliki perencanaan bagaimana mengelola jadwal yang dibuat untuk melakukan identifikasi risiko.

5.1.1.1.7 Rencana Pengelolaan Kualitas

Keseharian operasionalnya data center PT "X" telah memiliki standard kualitas yang harus dijaga sesuai dengan SLA (*Service Level Agreement*) yang dimiliki, untuk melakukan pengelolaan kualitas dari jasa PT "X", pengelolaan kualitas dilakukan dengan melakukan maintenance oleh tim facility yang setiap hari melakukan pengecekan pada setiap alat pendukung data center, begitu juga dengan personil keamanan yang di pekerjakan 24 jam dalam sehari, hal ini ditujukan untuk mencaga kualitas jasa data center yang diberikan oleh PT "X" .Dimana sistem tersebut tidak boleh down lebih dari 22 jam dalam satu tahun.

5.1.1.1.8 *Project Documents*

Dokumen proyek sebelumnya tidak dapat ditemukan dikarenakan, proyek identifikasi risiko ini belum pernah dilakukan oleh tim manajemen PT "X" dengan alasan PT "X" merupakan "pemain baru" dalam industri ini, yaitu baru memulai usahanya sejak 2003. namun dalam rentang waktu tersebut belum pernah dilakukan identifikasi risiko yang meninggalkan dokumen yang dapat dirujuk sebagai bahan identifikasi risiko selanjutnya.

"Dokumen apaan? Dokumen terdahulu? Ya nggak ada, kita kan baru kalo di data center, emang masih banyak kekurangannya. Kalo soal begituan kita akuin kita miss, nanti kan kita mau pindah nih ke lokasi baru yang lebih sesuai dengan standar data center, nanti disana deh kita benerin apa-apa yang masih kurang disini" (A.S 18 November)

5.1.1.1.9 Faktor Lingkungan yang memprngaruhi Perusahaan

Dalam melakukan identifikasi risiko, faktor yang mempengaruhi perusahaan harus dicatat sebagai bahan pertimbangan membuat risk register. Dalam Hal ini lagi,lagi PT "X" belum membuat daftar faktor yang mempengaruhi perusahaan dalam hal ini data center. Hal ini diindikasikan disebabkan oleh belum adanya tanggung jawab yang jelas untuk melakukan tahapan identifikasi risiko. Pihak Facility tidak merasa perlu membuatnya dikarenakan hanya sebagai eksekutor pemeliharaan peralatan.

"kalo soal dokumen kayak gitu jangan tanya ke facility lah, tanya AS atau tanya legal lah, atau kalau faktor-faktor begitu tanya anak salesnya aja,siapa tau mereka buat buat keperluan jualannya." (I.P 15 Februari 2012)

Ketika dikonfirmasi kepada tim sales, mereka juga tidak merasa bertanggung jawab dalam membuat faktor yang mempengaruhi perusahaan

"wah itu sih belum pernah bikin ya, soalnya kan udah hamper sama juga apa-apa aja yang jadi faktor sama apa yang ada di SWOT tapi seharusnya kalo terkait sama risiko mah soal faktor-faktor begitu aturan tanya si AS bukan? Kan dia tuh yang ngurusin SOP buat standarisasi aturan dy punya ya, jangan tanya sales" (Y.U 24 Maret 2012)

5.1.1.1.10 *Organizational Process Assets*

Aset proses yang dimiliki oleh PT “X” sudah didokumentasikan dengan baik, kecuali dokumen untuk keperluan identifikasi risiko yang tidak tersedia karena memang belum pernah dibuat sebelumnya. Aset proses yang dimiliki PT “X” mencakup form dan persyaratan akses masuk untuk pelanggan data center, dokumen data pelanggan. Untuk Bagan organisasi, PT “X” sudah memilikinya, namun alurnya masih tumpang tindih dan tidak efektif yang dapat menyebabkan chaos dalam pendelegasian tugas. Seperti yang dihadapi oleh pihak keamanan, dimana personel keamanan juga harus mengamankan aset perusahaan. Petugas keamanan tidak bertanggung jawab secara langsung kepada tim facility, pihak keamanan bertanggung jawab melaoprkan semua catatan ke manajer HRD dikarenakan semua personilnya merupakan tenaga outsource.

5.1.1.1.2 Alat membuat *Risk Register*

Ketika melakukan identifikasi risiko, PT “X” belum melakukan tahapannya dengan baik, namun untuk melakukan teknik pencatatan risiko yang dilakukan masih bersifat common sense, tidak dibuat berdasarkan input yang dibutuhkan PT “X” telah melakukan SWOT analisis. Namun deskripsi ini dibuat dan dipegang oleh tim marketing yang dijadikan bukan sebagai dasar pembuatan *risk register* namun untuk membuat analisa pasar, dan strategi pemasaran data center PT "X" analisa yang dibuat berupa analisa SWOT yang berisi kelemahan dan kelebihan dari data center PT “X”.

> "apaan? SWOT? kalo deskripsi kayak gitu mah, yang buat masih di tim marketing, biasan ya mereka buat buat liat kelemahan sama kelebihan data center kita, buat mereka bikin strategi marketing mereka lah," (8 Maret 2012)

5.1.1.1.3 *Risk Register Output*

5.1.1.1.3.1 Daftar risiko yang diidentifikasi

Hasil dari identifikasi risiko yang akan digunakan sebagai bahan analisa risiko merupakan daftar risiko yang diidentifikasi, dikarenakan PT “X” belum pernah melakukan upaya identifikasi risiko maka belum ada daftar risiko yang dapat diidentifikasi. Hal ini dikarenakan, PT “X” masih belum memperhatikan

hal-hal seperti ini dengan alasan merupakan pemain baru dalam industri ini, selain itu belum pernahnya kejadian pencurian data yang terjadi membuat PT "X" masih menganggap hal ini merupakan hal yang sepele. Dari hasil wawancara, peneliti juga mendapatkan kalau pihak-pihak terkait dalam operasional data center belum memahami apa fungsi identifikasi risiko dan apa saja tahapannya, hal ini dibuktikan dengan pandangan risiko untuk pencurian data hanya sebatas perampokan yang sudah pasti akan diketahui oleh PT "X"

> "Kita gak buat kayak begituan ya karena disini belum pernahlah ada kecurian kayak gitu, kalo ada kita pasti tau, lagipulan sekuriti kita juga jaga terus kok 24 jam,kalo ada yang ngerampok, ngambil paksa tuh server kan kita pasti taulah kalo soal akses masuk kan kita kasih form autorisasi yang harus diisi, kayak begitu kita juga udah meminimalisir risiko kan" (A.S 18 November 2011)

5.1.1.1.3.2 Daftar penanggulangan potensial yang dapat dilakukan

Sebelum membuat daftar rencana penanggulangan, harus terlebih dahulu memiliki daftar risiko yang diidentifikasi, karena PT "X" belum memiliki daftar risiko yang diidentifikasi berdasarkan input yang sudah disebutkan diatas, PT "X" juga belum memilikio daftar rencana penanggulangan yang dapat diterapkan untuk risiko. Penanggulangan yang ada saat ini masih berupa tindakan preventif dengan membuat prosedur akses, loading dan uloading barang dari data center dan juga pemeliharaan ruangan, belum ada daftar tindakan penanggulangan yang bersifat *recovery* jika risiko mempengaruhi operasional data center.

5.1.1.2 Rencana Manajemen Risiko

5.1.1.2.1 Rencana Management Risiko input

5.1.1.2.1.1 *Project Scope Statement*

Pernyataan lingkup proyek menjelaskan, secara rinci, hasil dari proyek dan pekerjaan yang diperlukan untuk membuat hasil tersebut dapat dicapai. Pernyataan lingkup proyek juga memberikan pemahaman umum dari ruang lingkup proyek antara para pemangku kepentingan proyek. Ini mungkin berisi pengecualian lingkup eksplisit yang dapat membantu dalam mengelola ekspektasi pemangku kepentingan. Ini memungkinkan tim proyek untuk melakukan perencanaan yang lebih rinci, memandu kerja tim proyek selama eksekusi, dan menyediakan dasar untuk mengevaluasi apakah permintaan untuk perubahan atau pekerjaan tambahan yang terkandung dalam atau di luar batas proyek. Dalam Hal ini PT "X"' belum melakukan deskripsi jelan mengenai ruang lingkup rencana manajemen risiko, divisi mana saja yang terlibat, semuanya masih berjalan secara normatif tidak didasarkan pada sebuah deksripsi mengenai ruang lingkup rencana manajemen risiko. Hal ini juga dikarenakan kurangnya pengetahuan pihak terkait mengenai apa itu Project Scope Statement

> "yang kamu maksud propject scope statement itu apa? Kan kita belum pernah buat analisa risiko begitu, ya kalo kamu tanya-embel-embelnya saya gak bisa kasih kekamu, disini semuanya masih by verbal aja, belum lengkaplah kalo soal begituan" (A.S 18 November 2011)

5.1.1.2.1.2 **Perencanaan Pengelolaan Biaya**

Perencanaan penegelolaan untuk melakukan manajemen risiko pada PT "X" belum dibuat terpisah dari biaya maintenance yang ada, seperti biaya identifikasi risiko yang belum dibuat begitupun dengan rencana pengelolaan biaya pelaksanaan manajemen risiko, belum dibuat karena manajemen risiko pada PT "X" belum dilaksanakan

> "biaya manajemen risiko? Gak ada itu sih, kita biaya pasti lah ada alokasi buat divisi facility, tapi itu buat biaya maintenance, itu buat preventif lah ya,

kita jaga AC, kita jaga CCTV supaya data center kita gak rusak kalo AC nya gak mati, supaya kita tetep bisa ngawasin pake CCTV, alokasi budget tahunan sih buat itu, selain buat maintenance ya juga buat beli-beli barang, kan tugas facility juga beli-beli barang peralatan, kita cari vendor ntar bikin PR , PO baru bayar. Kalo biaya sih paling yang kita keluarin buat itu aja" (I.P 15 Februai 2012)

Hal tersebut juga diamini oleh A.S selaku manajer assurance dimana, anggaran dana yang dibuat oleh PT "X" sudah mengalokasikan budget untuk melakukan manajemen risiko dengan memberli peralatan yang dapat mengurangi risiko

*"*kita sih kalo untuk risiko kita lebih prefer buat mengurangi ya, karena kalo dihilangkan nggak bisa dan kita juga gak mindahin risiko ke pihak ketiga atau asuransi, itu kan emang perusahaannya yang masukin asuransi sendiri kalo emang mau colo disini, kalo untuk ,mengurangi risiko kita menggunakan alat-alat yang canggih, untuk alat-alat itu kan kita bayar ya biaya manajemen risiko nya masuk kesitu lah" (A.S 18 November 2011)

5.1.1.2.1.3 Rencana Pengelolaan Jadwal

Jadwal pelaksanaan rencana manajemen risiko yang ada di PT "X" juga belum dibuat secara khusus, semua kegiatan perawatan dan operasional yang ada masih merupakan kegiatan sehari-hari yang akan terus dilakukan sampai ada perubahan peraturan dari manajemen, namun kegiatan tersebut tidak dapat dikategorikan dalam rencana manajemen risiko karena dilakukan tidak berdasarkan tahapan yang dibutuhkan untuk melakukan manajemen risiko.

"jadwal pemeliharaan? Jadwal sih yang di SOP itu kan kita ngejalanin tiap hari ya, dan kalo pemeliharaan gitu kan berkesinambungan bakal terus dilakuin kan, gak ada batesnya lah begitu, kecuali ada kebijakan dari manajemen buat menghentikan kegiatan tersebut, tapi ya gak mungkin lah masa melihara ada jadwalnya sampe kapan, ya dipelihara terus lah, kecuali pemelihaan sehari-hari tuh ada jadwalnya, pengecekan tiap jam berapa,

setiap 3 jam sekali suhu dipantau setiap seminggu dua kali ruangan di vakum nah itu ada jadwalnya." (I.P 15 Februari 2012)

5.1.1.2.1.4 *Communications Management Plan*

Rencana pengelolaan komunikasi. Rencana ini mendefinisikan interaksi yang akan terjadi pada proyek, dan menentukan siapa yang akan siap untuk berbagi informasi mengenai berbagai risiko dan tanggapan pada waktu yang berbeda (dan lokasi). Praktek yang telah dilakukan oleh PT "X" untuk interaksi antar divisi yang terkait dengan data center masih dilakukan via email secara personal,ataupun email. Untuk informasi yang harus diketahui oleh seluruh karyawan mengenai data center, informasi tersebut disebarkan lewat intranet oleh tim *internal communication*

"ya kalo penyampaian informasi SOP yang berkaitan sama data center nanti pak andi invite meeting orang-orang terkait lah, bisa juga lewat email, atau kalo emang semua harus tau kita upload di intranet, kan itu bisa dilihat, lagian semua SOP yang ada kan harus di upload di intranet kan, bisa juga minta bantuan internal communication" (I.P 15 Februari 2012)

5.1.1.2.1.5 *Enterprise Environmental Factors*

Faktor lingkungan perusahaan yang dapat mempengaruhi proses Rencana Manajemen Risiko menggambarkan tingkat risiko bahwa suatu organisasi akan bertahan. Seperti yang sudah disampaikan dalam analisa Faktor yang mempengaruhi Perusahaan yang dibutuhkan dalam membuat risk register, analisa faktor tersebut masih belum dibuat oleh manajemen PT "X"

5.1.1.2.1.6 *Organizational Process Assets*

Aset proses yang dimiliki oleh PT "X" sudah diterapkan, dalam pembuatan SOP dan dokumen lainnya, penjelasan tentang proses asset akan dibahas dalam bagian selanjutnya, sebagai input untuk membuat analisa risiko

"SOP yang ada ya, permit akses, gimana orang itu bisa masuk, harus terdaftar dalam form autorisasi, nanti kalo udah deal dia colo di kita kita

kasih PICnya form aoutorisasi, dia ngedaftarin 2 orang dari perusahaan tersebut yang diberikan kuasa buat masuk, melakukan maintenance kedalam ruang data center, itu isinya nama, identitas pake KTP juga, nanti dari tim facility akan buatin id log in dan paswordnya, nanti id dan lg in tersebut yang digunakan kalo dia masuk masuk kedalam ruang data center, jadi Cuma orang-orang itu aja yang boleh masuk. Selain itu juga kita ada SOP loading and unloading, gimana prosedur orang masukin dan mindahin server karena kan server dipindahin gak seenaknya aja, ada prosedurnya, SOP mah kita punya kok." (I.P 15 Februari 2012)

5.1.1.2.2 Teknik Rencana Manajemen Risiko

5.1.1.2.2.1 *Planning Meetings and Analysis*

Untuk melakukan analisa rencana manajemen risiko tim perlu melakukan meeting untuk mengembangkan rencana pengelolaan risiko. Untuk PT "X" meeting dilaksanakan secara berkala, baik meeting internal setiap divisi yang terkait, seperti meeting internal facility yang dilakukan setiap hari rabu, ataupun general meeting yang diadakan setiap hari senin.

"Pernah lah meeting internal, setiap hari rabu, meeting update gimana operasional, hambatan ada apa aja, selama seminggu ada kejadian apa, ada kerusakan apa nggak ya pasti ada meeting lah, nah kalo ada masalah yang melibatkan pihak lain ya nanti pak andi invite meeting divisi yang bersangkutan, lagipulan kan ada general meeting setiap hari senin, itu divisi-divisi lain juga ngumpul, sama presdir juga kan jadi kalo ada masalah yang krusial ya bisa dilempar ke floor disitu" (I.P 15 Februari 2012)

5.1.1.2.3 Hasil *Risk Management Plan*

5.1.1.2.3.1 Metodologi

PT "X" belum merasa penting untuk membuat perencanaan manajemen risiko, hal ini dibuktikan tidak dilakukannya pembuatan input yang memadai, hal ini

menyebabkan tidak adanya hasil yang sesuai, dalam hal ini metodologi. Metodologi dalam melakukan rencana manajemen risiko yang selama ini dipakai PT "X" memilih untuk mengurangi risiko dengan menggunakan peralatan yang canggih

> "kita sih kalo untuk risiko kita lebih prefer buat mengurangi ya, karena kalo dihilangkan nggak bisa dan kita juga gak mindahin risiko ke pihak ketiga atau asuransi, itu kan emang perusahaannya yang masukin asuransi sendiri kalo emang mau colo disini, kalo untuk ,mengurangi risiko kita menggunakan alat-alat yang canggih, untuk alat-alat itu kan kita bayar ya biaya manajemen risiko nya masuk kesitu lah" (A.S 18 November 2011)

5.1.1.2.3.2 Peran dan Tanggung Jawab

Rencana manajemen risiko dalam pelaksanaannya membutuhkan alur dan tanggung jawab yang jelas untuk setiap anggota tim. Untuk pembagian peran dan tanggung jawab, dikarenakan PT "X" belum membuat struktur tim untuk melaksanaan rencana manajemen risiko, maka dalam pelaksanaan pemeliharaan, keamanan data center PT "X" masih menggunakan organizational chart yang ada. Dalam organizational chart manajemennya sendiri PT "X" belum memiliki organizational chart yang efektif, hal ini dibuktikan dengan sekuriti yang dibawahi oleh Manajer HRD, hal ini dikarenakan para personil keamanan data center merupakan tenaga kerja outsource yang secara alur biroksrasi tidak jelas. Para personel keaman juga bekerja secara serebutan, karena tidak hanya mengamankan data center tapi juga mengamankan asset perusahaan

> "iya sih mbak, tugasnya gak terlalu ke sekuriti kalo saya rasa mah lebih berat ke admin, hahahaha. Oiya motor juga kesini ambil kuncinya. Kalo mau booking pake mobil juga kesini mbak telfonnya, nyari orang telfonnya juga kesini, ntar kuncinya dibalikin juga kesini lagi mbak kuncinya. udah gitu kan sekuriti kan kayak customer service juga, bikin report ada siapa aja yang dateng, dari branch juga lapornya kesini mbak" (AG 8 Maret 2012)

Selain terbentur masalah birokrasi, karena proses manajemen risiko belum terintegrasi, pekerjaan yang dilakukan juga masih banyak terjadi *overlapping* antar divisi, contohnya satpam yang seharusnya menjadi bagian dalam proses manajemen risiko dengan tugas mengamankan data center, PT "X" belum melakukan pemisahaan pekerjaan yang jelas, satpam di ruangan data center juga masih harus mengamankan aset perusahaan yang berakibat tidak fokusnya dalam menjalankan fungsi mengamankan data center.

5.1.1.2.3.3 Penganggaran

Untuk biaya operasional manajemen risiko yang dikeluarkan belum ada alokasi yang jelas, biaya untuk manajemen risiko ini masih disatukan dengan biaya perdivisi. Contohnya, biaya untuk melakukan maintanace peralatan di dalam ruangan data center masih masuk kedalam biaya operasional Divisi facility yang tidak dikategorikan kedalam biaya manajemen risiko.

> "biaya manajemen risiko? Gak ada itu sih, kita biaya pasti lah ada alokasi buat divisi facility, tapi itu buat biaya maintenance, itu buat preventif lah ya, kita jaga AC, kita jaga CCTV supaya data center kita gak rusak kalo AC nya gak mati, supaya kita tetep bisa ngawasin pake CCTV, alokasi budget tahunan sih buat itu, selain buat maintenance ya juga buat beli-beli barang, kan tugas facility juga beli-beli barang peralatan, kita cari vendor ntar bikin PR , PO baru bayar. Kalo biaya sih paling yang kita keluarin buat itu aja" (8 Maret 2012)

5.1.1.2.3.4 Estimasi Waktu

Selain biaya operasional, juga belum ada tabel waktu yang jelas sampai kapan manajemen risiko akan dilakukan, kegiatan yang dilakukan merupakan kegiatan rutin yang dilakukan sehari-hari dan akan terus dilakukan sampai ada perubahan peraturan baru dari pihak manajemen PT "X"

> "jadwal pemeliharaan? Jadwal sih yang di SOP itu kan kita ngejalanin tiap hari ya, dan kalo pemeliharaan gitu kan berkesinambungan bakal terus dilakuin kan, gak ada batesnya lah begitu, kecuali ada kebijakan dari manajemen buat menghentikan kegiatan tersebut, tapi ya gak mungkin lah masa melihara ada jadwalnya sampe kapan, ya dipelihara terus lah, kecuali

pemelihaan sehari-hari tuh ada jadwalnya, pengecekan tiap jam berapa, setiap 3 jam sekali suhu dipantau setiap seminggu dua kali ruangan di vakum nah itu ada jadwalnya." (8 Maret)

5.1.1.3 Project Scope Statement

5.1.1.3.1 *Project Scope Statement Input*

5.1.1.3.1.1 *Project Charter*

Project Charter memberikan deskripsi tingkatan tinggi proyek dan karakteristik produk. Hal ini juga berisi persyaratan persetujuan proyek. Jika sebuah project charter tidak digunakan dalamperusahaan, maka informasi yang sebanding perlu diperoleh atau dikembangkan, dan digunakan sebagai dasar untuk *project scope statement*. PT "X" belum membuat project charter yang terbukti belum adanya pembagian tanggung jawab yang jelas, tidak adanya alokasi anggaran yang dibuat untuk melakukan analisa riko.

5.1.1.3.1.2 *Requirements Documentation*

Dokumen-dokumen yang dibutuhkan dalam membuat *Project Statement* seperti SOP dan organizational proses asset lainnya, data center PT "X" telah memiliki beberapa SOP dalam operasionalnya, diantaranya SOP akses masuk, SOP loading dan unloading.

"SOP yang ada ya, permit akses, gimana orang itu bisa masuk, harus terdaftar dalam form autorisasi, nanti kalo udah deal dia colo di kita kita kasih PICnya form aoutorisasi, dia ngedaftarin 2 orang dari perusahaan tersebut yang diberikan kuasa buat masuk, melakukan maintenance kedalam ruang data center, itu isinya nama, identitas pake KTP juga, nanti dari tim facility akan buatin id log in dan paswordnya, nanti id dan lg in tersebut yang digunakan kalo dia masuk masuk kedalam ruang data center, jadi Cuma orang-orang itu aja yang boleh masuk. Selain itu juga kita ada SOP loading and unloading, gimana prosedur orang masukin dan mindahin server karena kan server dipindahin gak seenaknya aja, ada prosedurnya, SOP mah kita punya kok"

(I.P 15 Februari 2012)

5.1.1.3.2 Project Scope Statement Teknik

5.1.1.3.2.1 Product Analysis

Dalam membuat *Project Scope Statement* walaupun belum melakukan semua tahapan dengan baik, namun PT "X" sudah melakukan analisa produk, analisa produk ini dibuat oleh product manager, dalam hal ini product manager memiliki tugas untuk membuat product knowledge, analisa SWOT dan bertugas untuk mengupdatenya setiap sebulan sekali. Namun product manager untuk setiap product yang ada di PT "X" merupakan posisi baru.

> "ada sih kalo product analysis, itu yang bikin product manajernya, isinya tentang product knowledge, janji yang dikasih ke para calon customer apa, dan gimana cara mendeliver janji tersebut dengan baik, semua ntar yg handle si product manajer, tapi posisi itu kan baru, nanti tiap *produc*t punya PM sendiri" (Y.U 24 Maret 2012)

5.1.1.3.2.3 *Organizational Process Assets*

5.1.1.3.3 Hasil pendefinisian cakupan

5.1.1.3.3 .1 *Project Scope Statement*

Hasil dari pendefinisian cakupan proyek analisa risiko meliputi:

- Lingkup deskripsi produk

Deskripsi ini menguraikan karakteristik produk, jasa, atau hasil dalam project charter dan dokumentasi persyaratan, PT telah memiliki dokumen ini yang berbentuk product knowledge, deskripsi ini dibuat oleh product manajer ditujukan untuk keperluan menjual jasa *collocation.* Deskripsi ini meliputi rincian ruang data center, jumlah server yang dimiliki, spesifikasi peralatan yang digunakan.

- Kriteria penerimaan produk

Mendefinisikan proses dan kriteria untuk menerima produk,jasa, atau hasil yang telah dicapai. Kriteria yang harus dicapai dalam memenuhi layanan collocation, definisi tersebut hanya berbentuk SLA,*service level agreement* yang berisi perjanjai kerja, spesifikasi alat yang akan digunakan, maksimal downtime yang masih ditoleransi dan point-point lain yang harus dipenuhi PT "X"

5.1.1.4 Organizational Procces Assets

Untuk melakukan analisa risiko, selain input yang sudah disebutkan sebelumnya, juga dibutuhkan Organizational Process Assets, yang meliputi SOP, PT "X" telah memiliki beberapa SOP khusus untuk keamanan data center,

> "SOP yang ada ya, permit akses, gimana orang itu bisa masuk, harus terdaftar dalam form autorisasi, nanti kalo udah deal dia colo di kita kita kasih PICnya form aoutorisasi, dia ngedaftarin 2 orang dari perusahaan tersebut yang diberikan kuasa buat masuk, melakukan maintenance kedalam ruang data center, itu isinya nama, identitas pake KTP juga, nanti dari tim facility akan buatin id log in dan paswordnya, nanti id dan lg in tersebut yang digunakan kalo dia masuk masuk kedalam ruang data center, jadi Cuma orang-orang itu aja yang boleh masuk. Selain itu juga kita ada SOP loading and unloading, gimana prosedur orang masukin dan mindahin server karena kan server dipindahin gak seenaknya aja, ada prosedurnya, SOP mah kita punya kok." (15 Februari 2012)

> Ketika ditanyakan, pihak keamanan PT "X" telah memiliki pengetahuan yang baik akan SOP yang harus dijalankan, hal itu terbukti dari yang peneliti lihat dilapangan dimana keamanan PT "X" tetap menjalankan SOP untuk memberikan instruksi kepada pengunjung yang datang untuk mengisi log in buku tamu walaupun orang tersebut telah sering datang ke data center PT "X"

> "misalnya kan customer kita PT X (menyebutkan nama perusahaan telekomunikasi asal china) kalo dulu kan kalo buat masuknya kan dia nulisnya manual tuh mbak nulis di formnya. Kalo sekarang tuh datanya diminta dulu sama Pak Andi , nanti pak Andi yang proses buat email sama

log in masuk ke data centernya, kan ini ada log in elektronik nih mbak, itu tuh computer yang itu (menunjuk ke computer yang ada didepan) jadi ntar kalo dia dating dia tinggal masukin id sama password yang udah dikasi sama pak Andi" (A.G 8 Maret 2012)"

Selain SOP Data Center PT "X" juga memiliki dokumen terkait yang digunakan untuk tujuan pengamanan data center, dokumen tersebut adalah Daftar kunci dan nomer rack customer,dan daftar customer yang merubah paswordnya. Daftar tersebut dibuat oleh tim facility dan diberikan ke sekuriti sebagai alat mereke mengamankan data center.

"kalo ini kita dikasih tau sama facility sih mbak, itu kan tadi udah ada daftarnya tuh, kunci nomer berapa rack nomer berapa" (A.G 8 Maret 2012)

Mengenai persyaratan komunikasi, pihak data center masih bekerjasama dengan pihak corporate communication untuk mempublikasi kebijakan-kebijakan yang ada, untuk eksternal maupun internal.

"ya kalo penyampaian informasi SOP yang berkaitan sama data center nanti pak andi invite meeting orang-orang terkait lah, bisa juga lewat email, atau kalo emang semua harus tau kita upload di intranet, kan itu bisa dilihat, lagian semua SOP yang ada kan harus di upload di intranet kan, bisa juga minta bantuan internal communication" (I.P 15 Februari 2012)

Sedangkan prosedur pengawasan keuangan (misalnya, waktu pelaporan, pengeluaran yang diperlukan dan ulasan pencairan, kode akuntansi, dan ketentuan kontrak standar) masih dilakukan oleh pihak *finance* PT "X". Organizational Process Assets juga berisi Informasi historis (misalnya, proyek catatan dan dokumen, semua penutupan proyek informasi dan dokumentasi, informasi tentang hasil proyek sebelumnya dan informasi kinerja proyek sebelumnya, dan informasi dari upaya manajemen risiko), PT "X" belum melakukan dokumentasi yang baik berkenaan dengan catatan historis ini, mengenai hasil proyek sebelumnya tidak bisa didapat karena belum pernah dilakukannya analisa risiko,hal ini peneliti peroleh dari hasil wawancara dengan AG, salah satu staff keamanan:

"Disini belum ada yang namanya project manager, kalo soal keamanan ya lapornya masih ke HRD yang ngebawahin semua satpam, soalnya kan satpam disini outsource semua jadi atasannya masih langsung ke HRD mbak" (8 Maret 2012)

Selain terbentur masalah birokrasi, karena proses manajemen risiko belum terintegrasi, pekerjaan yang dilakukan juga masih banyak terjadi *overlapping* antar divisi, contohnya satpam yang seharusnya menjadi bagian dalam proses manajemen risiko dengan tugas mengamankan data center, PT "X" belum melakukan pemisahaan pekerjaan yang jelas, satpam di ruangan data center juga masih harus mengamankan aset perusahaan yang berakibat tidak fokusnya dalam menjalankan fungsi mengamankan data center, seperti yang dikeluhkan oleh AG:

" iya sih mbak, tugasnya gak terlalu ke sekuriti kalo saya rasa mah lebih berat ke admin, hahahaha. Oiya motor juga kesini ambil kuncinya. Kalo mau booking pake mobil juga kesini mbak telfonnya, nyari orang telfonnya juga kesini, ntar kuncinya dibalikin juga kesini lagi mbak kuncinya" (8 Maret 2012)

5.1.2 Teknik Analisa Risiko

Dari beberapa pilihan teknik analisa risiko yang dapat dilakukan setelah mengumpulkan input, karena PT "X" belum melakukan proses pengumpulan input yang dibutuhkan dengan baik untuk melakukan analisa risiko, hal ini menyebabkan belum adanya teknik analisa spesifik yang digunakan oleh PT "X" jika dilihat dari apa yang dilakukan dilapangan berkaitan dengan analisa risiko,namun jika dilihat pada operasional kesehariannya PT "X" menggunakan teknik analisa risiko yang paling mendekati dengan teknik penilaian tingkat urgensi risiko. Dalam analisa risiko kualitatif risiko dapat dimasukan kedalam peringkat sesuai dengan tingkat urgensinya, untuk hal ini PT "X" telah melakukannya dengan melakukan respon terhadap area yang paling urgen untuk diatasi terlebih dahulu seperti mengamankan pintu masuk dan menggunakan alat pemantau setiap orang yang masuk kedalam ruangan data center. Analisa risiko dengan teknik analisa urgensi ini melihat area risiko yang oaling membutuhkan respon secara cepat, hal ini seperti yang dikemukakan oleh A.S:

> "untuk bikin analisa risiko kita sih masih liat tingkat urgensi hal tersebut, kalo kayak akses masuk itu kan hal yang paling berisiko ya karena bersinggungan langsung dengan alat-alat di ruang data center, jadi itu duluan yang jadi prioritas kita" (8 Maret 2012)

Walaupun PT "X" telah mencoba untuk membuat analisa risiko dengan cara membagi risiko kedalam beberapa tingkatan, namun tingkat urgensi tersebut lagi-lagi tidak dibuat berdasarkan hasil input yang dibutuhkan,namun hanya secara *common sense.* Hal ini sangat berbahaya karena jika tidak membuat skala urgensi risiko dengan mendasar kepada input yang dibutuhkan maka hasil yang dicapai akan kemungkinan besar tidak sesuai. Sebagai contoh PT "X" tidak melakukan analisa urgensi risiko dengan melihat biaya yang ditimbulkan jika risiko tersebut muncul, jika tingkat risiko yang dibuat tidak mengacu pada biaya yang ditimbulkan risiko bisa saja PT "X" akan salah membuat tingkatan urgensi risiko yang membuat risiko yang justru memiliki tingkat urgensi tinggi namun tidak dikategorikan penting dan tidak segera diatasi yang akan mengakibatkan PT "X" menderita kerugian finansial.

5.1.3 Hasil Analisa Risiko

5.1.3.1 Risk Register yang telah diperbaharui

Setelah melakukan tahapan, mengumpulkan input dan memilih teknik analisa risiko, maka hasil yang akan didapat sesuai yang dikemukakan oleh buku *A Guide To the Project Management Body of Knowledge Fourth Edition* adalah risk register yang telah diperbaharui, dikarenakan risk register di awal yang dibutuhkan sebagai input untuk melakukan analisa risiko juga belum dibuat sesuai dengan kriteria yang harus dipenuhi untuk membuat risk register, maka analisa risiko belum dapat dilakukan dengan baik sehingga risk register juga tidak dapat diperbaharui. Hasil analisa risiko yang ada hanyalah berbentuk catatan dan laporan seperti daftar kegiatan pemeliharaan peralatan,daftar tamu pelanggan yang datang yang berisi waktu masuk,keluar,dan kegiatan yang dilakukan didalam data center. Sampai saat ini dari catatan inilah yang berkapasitas untuk dijadikan dasar sebagai pembuat keputusan apakah perlu ada perubahan dengan proses pengamanan data center.

BAB VI

PENUTUP

6.1 Kesimpulan

Dalam melakukan operasionalnya, PT "X" menggunakan alat-alat yang digunakan untuk mengurangi risiko, namun dalam penentuan penggunaan alat-alat tersebut dan beberapa proses lain seperti pengecekan seraca rutin,proses pemberian akses masuk kedalam ruang data center PT "X" belum mengacu pada hasil analisa risiko yang dijalankan dengan baik sesuai dengan tahapan analisa risiko menurut literature yang digunakan oleh peneliti yaitu, tahapan analisa risiko yang dikemukakan oleh Project Institute dalam buku *A Guide To the Project Management Body of Knowledge Fourth Edition*. Pada penilaian risiko menurut tahapan yang dikemukakan oleh buku *Project Institute* hasil yang seharusnya didapat setelah melakukan analisa risiko kualitatif adalah risk register yang telah diperbaharui,namun PT "X" belum melakukan penilaian risiko karena dalam penelitian ini tidak terdapatnya atau tidak diberikanya data pasti mengenai kejahatan yang pernah terjadi atau kehilangan data yang pernah terjadi. Dengan tidak adanya data ini, PT "X" tentunya akan mengalami kesulitan dalam melakukan penilaian risiko. Dampak dari tidak berjalanya proses manajemen risiko terlihat dalam pelaksanaan operasional. Banyak dokumen dalam pembuatan risk register yang tidak dijalankan dengan baik seperti biaya yang ditimbulkan akibat risiko, stake holder yang berisi peran,tanggung jawab *stakeholder* baik internal maupun eksternal. Hanya ada *stakeholder register* berupa SLA yang diberlakukan untuk pelanggan.

Begitu juga untuk tahapan membuat Rencana manajemen risiko, belum dilakukan sesuai dengan proses pembuatan rencana manajemen risiko yang baik. Tidak adanya *Person In Charge* untuk memonitor pelaksanaan manajemen risiko yang ada, tidak dibuatnya jadwal pelaksanaan manajemen risiko. Hal ini

mengakibatkan rencana manajemen risiko yang dibuat tidak dapat dijadikan masukan untuk pembuatan analisa risiko.

Dari berbagai masukan yang dibutuhkan untuk melakukan analisa risiko tidak tersedia, hal tersebut menjadi hambatan bagi PT "X" untuk melakukan analisa risiko, sehingga teknik analisa risiko yang dijalankan oleh PT "X" dilakukan berdasarkan pengamatan *common sense* yang tidak dapat dipertanggung jawabkan. Hal ini sangat berbahaya bagi kelangsungan operasional data center karena dapat menimbulkan kerugian jika tindakan mitigasi yang dilakukan tidak sesuai dengan realita dampak yang disebabkan oleh risiko yang terjadi dilapangan.

Analisa risiko kualitatif akan menghasilkan risk register yang telah diperbaharui, namun dikarenakan tahapan analisa risiko tidak dilakukan sesuai dengan tahapan yang seharusnya, maka hasil analisa risiko yang dimiliki oleh PT "X" tidak berupa risk register yang diperbaharui, namun hanya berupa catatan yang dimiliki oleh pihak-pihak terkait. Dengan tidak dilakukannya tahapan analisa risiko dengan baik, hal ini akan berpengaruh kepada operasional data center PT "X" Risiko yang tidak teridentifikasi dan tidak diklasifikasikan kedalam tingkat urgensi sesuai dengan waktu dan dampak yang akan ditimbulkan akan mengakibatkan kerugian financial.

DAFTAR PUSTAKA

Buku:

Andy,Jones. (2005). *Risk Management For Computer Security*. USA:Elsevier Inc

Bungin, Burhan. (2003). *Analisis Data Penelitian Kualitatif; Pemahaman filosofis dan Metodologis ke Arah Penguasaan Model Aplikasi*. Jakarta: PT.Raja Grafindo Persada.

Charles,Yoe. (2012). *Primer On Risk Analysis Decision Making Under Uncertainty*. USA: CRC Press

Evan,Wheeler et all. (2011). *Security Risk Management Building an Information Security Risk Management Program from the Ground Up*. USA: Else vier Inc

HermaN,Kruegle. (2007). *CCTV Surveillance Analog and Digital Video Practices and Technology*. USA: Elsevier, Inc

John,Magnabosco. (2009). *Protecting SQL Server Data*. USA:Simple Talk Publishing

Joko Subagyo. (2005). *Metode penelitian dalam teori dan praktek*. Jakarta: Rinekacipta

Kountur, Ronny. (2003). *Metode Penelitian Untuk Penelitian Skripsi dan Thesis*. Jakarta : Penerbit PPM

Koentjaraningrat. (1997). *Metode Penelitian Masyarakat*. Jakarta: Gramedia.

Krutz, R.L,et all. (2003). *The CISSP® Prep Guide: Gold Edition*. USA: John Wiley Publising

Lawrence, J Fenelly. (2004). *Effective Physical Security*. USA: Elsevier Inc

Lexy J moleong, (2006) *Metodoligi penelitian Kualitatif*. Bandung: Rosdakarya

Mauricio Arregoces (2005) *Data Center Fundamentals*. USA: Cisco Press

Milan Petkovi´c,et all (2006). *Security, Privacy,and Trust in Modern Data Management*. New York: Springer Berlin Heidelberg

National Crime Prevention Institute. (2001). *Understanding Crime Prevention,Second Edition*. Kentucky: National Crime Prevention Institute.

Neuman, W Lawrence. (2003). *Social research Methods, Qualitative and Quantitative Approach. Fifth Edition*. NewYork: Allyn & Bacon

Project Management Institute. (2008). *A Guide To the Project Management Body of Knowledge Fourth Edition*. USA: Project Management Institute, Inc

Suryabrata, Sumadi. (2000). *Metode Penelitian*. Jakarta: Rajawalipress.

Sugiyono. (2004) *Memahami Penelitian Kualitatif*. Bandung: Alfabeta

Tarek,Saadawi et all. (2011). *Cyber Infrastucture Protection*. USA: Strategic Studies Institute

Thomas,Norman. (2003). *Risk Analysis and Security Counter measure Selection*. London: CRC Press

W.Lawrence,NewmaN. (2007). *Basic Of Social Research Qualitative and Quantitative approaches*. USA: Pearson Education, Inc

Jurnal:

Rex Kelly Rainer, Jr., Charles A. Snyder, Houston H. Carr (2002) *Risk Analysis for Information Technology Risk Analysis for Information Technology*

http://www.jstor.org/stable/40397977

K Muralidhar (1999). *A General Additive Data Perturbation Method for Database Security*

http://www.jstor.org/discover/10.2307/2634846?uid=3738224&uid=2&uid=4&sid=56237432173

Wang, Richard Y; Strong, Diane M *(2003) Beyond Accuracy: What Data Quality Means to Data Consumers*

Roger Needham (2002). *The Clifford Paterson Lecture, 2002 Computer Security? Effects of Closed-Circuit Television on Crime*

http://www.jstor.org/stable/3559260

Paul M. Schwartz and Edward J. Janger (2001). *Notification of Data Security Breaches*

http://www.jstor.org/stable/40041541

Bomil Suh and Ingoo Han (2000). *The Impact of Customer Trust and Perception of Security Control on the Acceptance ofElectronic Commerce*

http://www.jstor.org/stable/27751068

Ioannis V. Koskosas and Ray J. Paul (2003). *Information Security Management in the Context of Goal-Setting.*

http://www.jstor.org/stable/3867932

C. Satapathy *(2002). Law for Computer Misuse and Data Protection*

http://www.jstor.org/stable/4407262

Rein Turn, Norman Z. Shapiro, Mario L. Juncosa (2001). *Privacy and Security in Centralized vs. Decentralized Databank Systems*

http://www.jstor.org/stable/4531626 .

Internet

http://lifestyle.okezone.com/read/2009/02/26/55/196468/karyawan-sakit-hati-berpotensi-curi-data-perusahaan

"XL Akui Upaya Pencurian Data oleh Oknum Asing" diakses melalui

http://teknologi.vivanews.com/news/read/41074xl_akui_upaya_pencurian_data_oknum_asing Pada 2 November 2011, 09.35 WIB

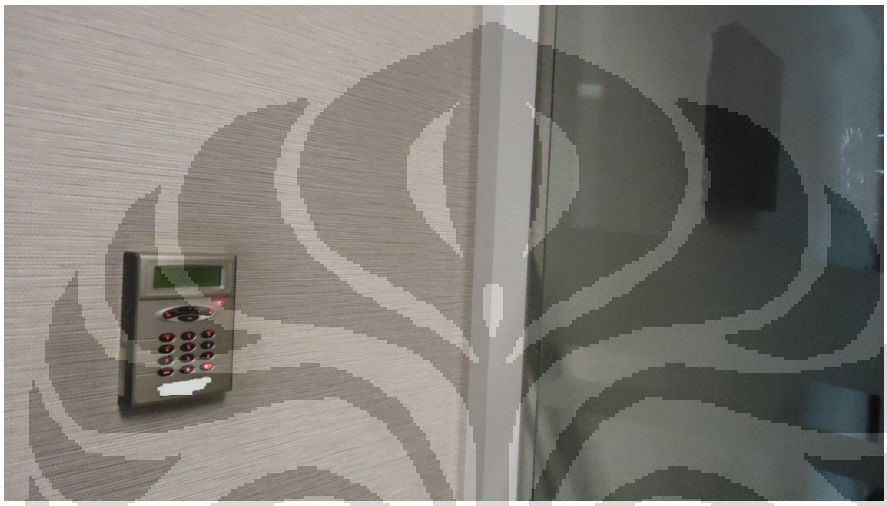
"Jangan Abaikan Pencurian Data oleh Orang Dalam" diakses melalui http://tekno.kompas.com/read/2008/12/10/03412610/jangan.abaikan.pencurian.data.oleh.orang.dalam Pada 16 November 2011, 17.00 WIB

Wow, Transaksi Pencurian Data Tembus Miliaran Dolar diakses melalui http://inet.detik.com/read/2011/12/15/184152/1792282/323/wow-transaksi-pencurian data-tembus-miliaran-dolar pada 16 Januari 22.00 WIB 2012

Lampiran 1

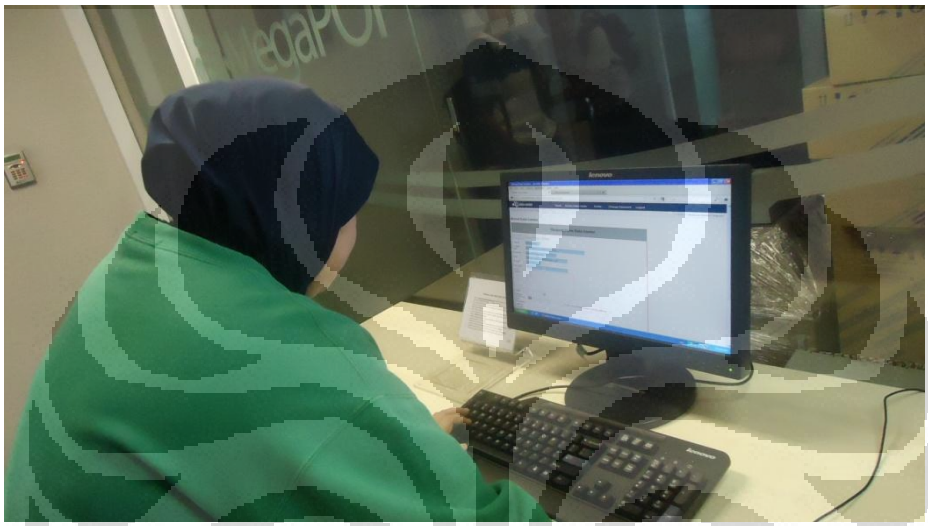
Gambar-gambar Ruang Data Center

ID Card pada Pintu Masuk Ruang Data Center

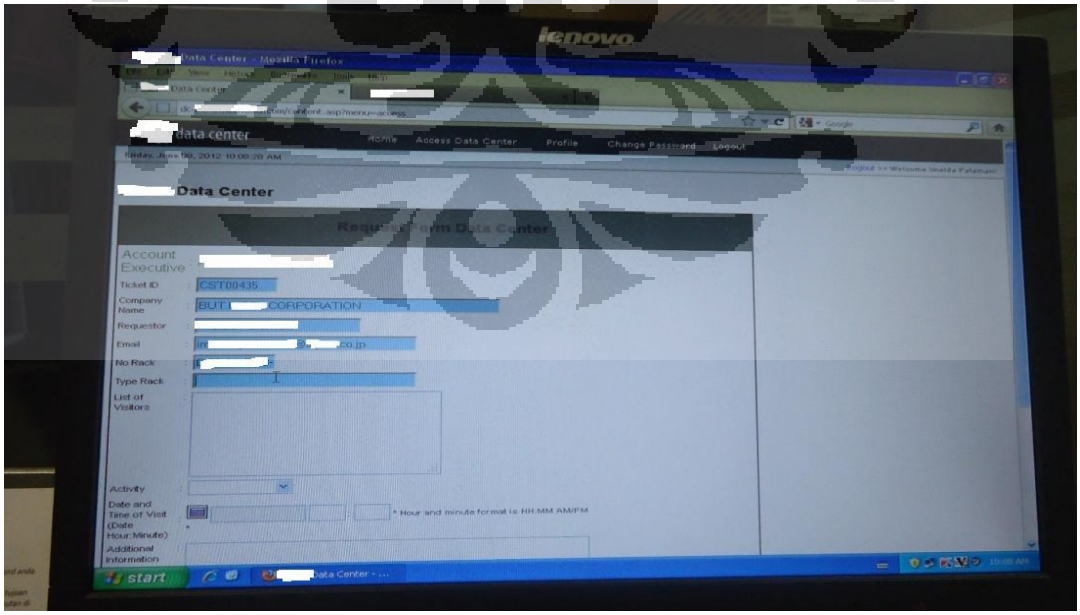


CCTV di depan ruang data center

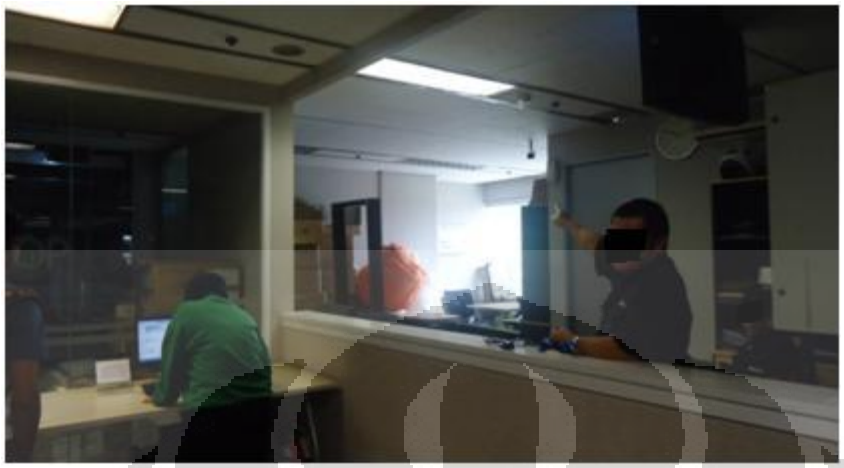
Pengunjung Mengisi Log in Elektronik melalui Personal Computer di depan Ruang Data Center



Tampilan Log in Data Center



Ruang Sekuriti didepan pintu masuk data center



ID Card

unloading equipment form

general

Nama Perusahaan *Company Name*	
Tanggal *Date*	
Data Center ID #	

declaration

Warranties

Although the best efforts are made to ensure that the information in this document is complete and correc makes no warranty of any kind with regards to this equipment.
Information in this document is correct at date of completion, and shall not be liable for errors contained herein or for incidental or consequential damages with the furnishing, performance, or use of this equipment.

Non-disclosure

Information contained in this document is intended for use by staff and customers. This information must not be disclosed to competitors without the express written consent of

introduction

Nama Pelanggan *Client Representative*	
Jabatan *Title*	
KTP/Passport ID #	
Note :	
Tanda Tangan *Signature*	

LAMPIRAN 4

Pedoman Wawancara

1. Gambaran umum data center PT "X" dari sejarah, luas ruangan, asset yang dimiliki
2. Bagaimana penerapan prosedur pengamanann?
3. Apa ada SOP terkait dengan data center? Kalau ada sebutkan
4. Bagaimana penggunaan alat-alat pengamanan seprti CCTV?
5. Hambatan dalam melaksanakan pengamanan?
6. Apakah ada dokumen-dokumen lain yang dipakai sebagai bahan melakukan analisa risiko?
7. Birokrasi dalam melakukan keamanan data center?
8. Perencanaan jadwal dalam melaksanakan analisis risiko?
9. Apakah ada alokasi anggaran untuk melakukan analisa risiko?
10. Bentuk menejemen risiko apa yang dilakukan?
11. Apakah ada SWOT analisa?
12. Apakah ada data deksripsi faktor-faktor yang mempengaruhi operasional data center?

LAMPIRAN 5

Wawancara dengan IP, staf facility data center PT "X" pada tanggal 15 Februari 2012 pada pukul 17.30 WIB

P: Peneliti

I:Informan

P: pak IP, mau nanya-nanya nih, kan udah janji mau ngebantuin gua kan

I: yailah nanya apaan sih? Yaudah sini aja veg nanya-nanya, udah kayak paling pinter aja gua ditanya-tanya

P:woelah, pinterlah kalo gak pinter masa masuk sini, ahahahaha bagi goceng! Kan udah gua puji lo pak

I: dasar lo, mau nanya apaan?

P: mau nanya-nanya soal data center lah, masa gua mau nanya hobi lo apaan, biar pinteran dikit gitu gua tau yang begituan

I: kenapa data center?

P: asset kita apaan aja sih yang ada di data center?

I: asset? Yang kayak gimana nih yang lo maksud?

P: ya asset, didalem data center tuh ada apa aja barang-barang berharganya?

I: yang jelas kagak ada emas,kagak ada berlian

P: woelah pak IP, serius napa dah, gua kasih donat juga ah lo biar serius,ahahaha

I:ahahaha, iya dah, di data center ya ada, AC, ada server, kita punya UPS juga, ada juga FM 200, ada juga CCTV, UTP,switch,firewall, nah tuh ngarti kagak lo?

P: wets ngartilah, demi kemajuan PT "X" gua udah privat niar ngerti begituan, ngahahahahha. Itu merknya apaan aja pak?

I:kalo AC kita pake libert, itu AC khusus data center, kita punya 4 tuh kalo itu, di DC 1 ada 1, di DC 2 ada 1 di DC 3 ada 2

P: itu khusus data center tuh AC? Emang kagak bisa pake daikin aja apa?

I:bisa sih bisa tapi ya terlalu beresiko lah pake AC daikin, lo kata itu ruang tamu tempat lo ngadem anginya sepoy-sepoy lo pakein AC begituan? Data center mana bisa lah, kalo data center itu suhunya paling bawah plus minus 16 derajat, kalo dibawah 16 nanti bisa berembun kalo ada air bisa korslet kalo batas atasnya di plus minus 21, kalo diatas itu bisa nyala tuh si FM 200

P: fm 200 itu apaan?

I: Itu alat pemadam kebakaran, kalo dia ngedeteksi panas, nanti dia ngeluarin gas fm 200, langsung menghisap oksigen supaya gak jadi kebakaran, makanya kalo itu diaktifin gak boleh ada manusia didalem sini.

P: ooh gitu, nah kalo rack yang kita pake kita pake apa aja?

I: kita pake rack tuh rack dari IBM ada, fujitsu juga ada, ntar deh gw kasih listnya sama lo, mana si email lo jangan kayak orang susah dah ada email masih nanya konvensional begini

P: woelah kayak begini lebih akurat! Kalo lo gak jawab kan bis gw injek kaki lo pak biar jawab, ahahahaha.

Yauidah itu beneran ntar lo email yak

I: iyee ntar gua email pegaa, kalo kagak kan lo tingal treakin secara meja lo didepan gua

P: pak kalo dilihat dari klasifikasinya, data center ini tier berapa sih?

I: ini tier 2

P: hah kok tier 2? Emang klasifikasi tier 2 itu gimana sih pak?

I: iya ini tier 2 kan kita udah ada redundant, maksudnya itu kita ada back up nya, kalo kita mati kan kita ada back up dr cabang, kalo listrik kita ada UPS yang bisa

nahan 3 jam sebelum listrik PLN nyala, lantai kita juga raised floor dan data center kita kan ditujukan buat keperluan perusahaan,soalnya kan ini gedung kita jadi tenat, gak berdiri sendiri buat data center,data center yang baik mah gak digedung perkatoran. Nah kalo data center tier 4, dia harus punya back up power pesaing PLN, yang sebesar itu dayanya di Indonesia belum ada tier 4

P: eh pak, itu lo ngejalanin operasional data center ada SOPnya gak sih? Lo bikin daftar risiko yang lo adepin selama ngejalanin operasional data center gak? Secara itu kan data orang didalemnya

I: SOP mah ada, kan kalo orang dateng harus isi form, harus terdaftar di form authorize segala macem itu SOP juga kali, gimana sih lo.

P: hooo, bole bole, kalo SOP yang lain ada kagak? Kayak SOP lo harus ngebersihin tuh ruangan berapa kali dalam sehari, suhunya berapa

I: SOP maintenance ya adalah, sehari tuh harus dicek suhunya pertiaga jam itu ruangan juga harus dibersihin, harus di vakum karena gak bisa dipel kan, tapi harus dust clear.

P: nah ngomong-ngomong ngebersihin, itu si soribin punya akses masuk yak? Gila gua aja gak bisa masuk

I: iya bisa masuk, kan dia bersih-bersih tapi dia masuk juga gak sendiri lah, asistensi orang dari facility salah-salah dia nyenggol kabel kan bisa berabe.

P: nah kan lo gak pernah bikin identifikasi risiko nih, trus gimana lo ngejalanin operasional lo dengan baik pak, maksud gw kan kalo lo udah bikin identifikasi risiko lo tau tuh mana-mana aja yang bisa mnegancam operasional data center

I: lah kan bagian-bagian yang berisiko kayak keamanan, udah dibuatin SOPnya, palingan kalo kayak gitu apa sih risikonya, orang luar kan, nah itu udah kita identifikasi terus kita tindak lanjuti dengan membuat SOP keamanan itu, jadi orang dateng harus lapor, harus ada terdaftar di form autorisasi, kasih KTP, risiko apalagi emangnya? Risiko orang jelek kayak lo iya

P: parah banget lo yeee,emangnya belom pernah apa pak dari manajemen bikini proyek analisa risiko gitu? Kalo analisa risiko kan diawali identifikasi risiko, kaloo risikonya udah diidentifikasi bisa deh bikin analisa risikonya biar ketauan apa-apa aja yang harus diperhatiin

I: wah kalo kayak gitu mah lo Tanya AS noh yang bikin-bikin risk assessment segala macem, tapi setau gua sih kayak gitu belum ada ya, kit ngejalanin apa yang keliatan aja, apa yang gak keliatan ya berarti bukan risiko lah, asumsi awalnya kayak gitu lah ya.

P: nah kalo biaya, ada gak biaya yang di alokasiin buat manajemen risiko?

I: biaya manajemen risiko? Gak ada itu sih, kita biaya pasti lah ada alokasi buat divisi facility, tapi itu buat biaya maintenance, itu buat preventif lah ya, kita jaga AC, kita jaga CCTV supaya data center kita gak rusak kalo AC nya gak mati, supaya kita tetep bisa ngawasin pake CCTV, alokasi budget tahunan sih buat itu, selain buat maintenance ya juga buat beli-beli barang, kan tugas facility juga beli-beli barang peralatan, kita cari vendor ntar bikin PR , PO baru bayar. Kalo biaya sih paling yang kita keluarin buat itu aja

P: itu dalem setahun alokasinya berapa tuh pak?

I: wah gede itu mah, gua gak tau itu mah confidential lah, kalo itu lo Tanya pak andi dah

P: tapi ada kan tuh alokasi biaya yang digunain buat ngelola risiko?

I: ya ada, kita sih gak bilang itu buat ngelola risiko ya, itu biaya buat pemeliharaan, tapi dengan terpelihara dengan baiknya semua asset yang kita punya kan secara langsung juga mengurangi risiko kehilangan,kerusakan dan lain-lain dong

P: kalo jangka waktu pengelolaan atau maintenance itu ada gak pak?

I: jadwal pemeliharaan? Jadwal sih yang di SOP itu kan kita ngejalanin tiap hari ya, dan kalo pemeliharaan gitu kan berkesinambungan bakal terus dilakuin kan, gak ada batesnya lah begitu, kecuali ada kebijakan dari manajemen buat menghentikan kegiatan tersebut, tapi ya gak mungkin lah masa melihara ada jadwalnya sampe

kapan, ya dipelihara terus lah, kecuali pemelihaan sehari-hari tuh ada jadwalnya, pengecekan tiap jam berapa, setiap 3 jam sekali suhu dipantau setiap seminggu dua kali ruangan di vakum nah itu ada jadwalnya.

P: ini semua kegiatan lo harus lapor sama pak andi semuaya pak IP? Di tim lo ada pembagian tugas gak sih?

I: Iya, ini semua dilaporinnya ke pak andi semua kegiatannya ngapain aja, paling nggak dia tau lah, dia kan juga mantau tuh pemeliharaan gimana, kalo soal pembagian tugas ya pasti ada lah, gw nih focus ke data center, cek AC, cek kelembaban gitu-gitu deh, tapi kadang juga masih disuruh ngebenerin pintu yang rusak, disini kan emang gitu gak bisa ngeliat orang nganggur.

P: itu pembagian tugasnya udah pas tuh pak? Jelas alur tanggung jawabnya?

I: ya jelas lah, kan lapornya ke pak andi, kalo kita sih satu tim ya namanya tim kerja bareng lah kalo ada yang kurang tenaga kita back up juga

P: itu kan pasti ada SOP yang harus dikasih tau antar divisi tuh, kayak syarat kalo mau masuk gimana kan harus ada, itu penyampaiannya pake apa?

I: ya kalo penyampaian informasi SOP yang berkaitan sama data center nanti pak andi invite meeting orang-orang terkait lah, bisa juga lewat email, atau kalo emang semua harus tau kita upload di intranet, kan itu bisa dilihat, lagian semua SOP yang ada kan harus di upload di intranet kan, bisa juga minta bantuan internal communication

P: pak kalo ngebahas data center pernah meeting gak?

I: pernah lah meeting internal, setiap hari rabu, meeting update gimana operasional, hambatan ada apa aja, selama seminggu ada kejadian apa, ada kerusakan apa nggak ya pasti ada meeting lah, nah kalo ada masalah yang melibatkan pihak lain ya nanti pak andi invite meeting divisi yang bersangkutan, lagipulan kan ada general meeting

setiap hari senin, itu divisi-divisi lain juga ngumpul, sama presdir juga kan jadi kalo ada masalah yang krusial ya bisa dilempar ke floor disitu.

P: jadi SOP yang facility punya menyangkut data center apa aja pak?

I: SOP yang ada ya, permit akses, gimana orang itu bisa masuk, harus terdaftar dalam form autorisasi, nanti kalo udah deal dia colo di kita kita kasih PICnya form aoutorisasi, dia ngedaftarin 2 orang dari perusahaan tersebut yang diberikan kuasa buat masuk, melakukan maintenance kedalam ruang data center, itu isinya nama, identitas pake KTP juga, nanti dari tim facility akan buatin id log in dan paswordnya, nanti id dan lg in tersebut yang digunakan kalo dia masuk masuk kedalam ruang data center, jadi Cuma orang-orang itu aja yang boleh masuk. Selain itu juga kita ada SOP loading and unloading, gimana prosedur orang masukin dan mindahin server karena kan server dipindahin gak seenaknya aja, ada prosedurnya, SOP mah kita punya kok.

P: selain itu dokumennya apa lagi pak yang terkait sama data center?

I: kita juga ada daftar kunci sesuai nomer racknya, berapa besar dua pake colocation kita, itu daftar juga kita share ke sekuriti jadi sekuriti bisa nyontek tuh daftar kalo ada customer yang dateng, kita juga ada daftar customer yang melakukan update password, nah data tersebut juga kita share ke sekuriti supaya bisa jaga-jaga aja, siapa aj yang gak bisa masuk kalo masih pake password lama. Kita kan bukan Cuma jual keamanan secara fisik ya tapi juga secara mental, itu aotorisasi juga kita update terus jangan sampe orang yang udah keluar tapi masih punya akses permit masih bisa masuk, itu kan bahaya.

P: itu di data center, kalo mereka utak-atik pake computer kan ya pak? Itu data apaan sih?

I: iya pake laptop, ya banyak lah data mereka itu sih hak mereka mau taro data apa, yang jelas kan itu data confidential mereka, segala aplikasi dan lain-lain tapi datanya mah bukan data mentah di exel gitu, itu data udah di enskripsi, bentuknya udah berupa logika dan config aja, jadi kalo yang ngambil orang awam juga dia gak bisa baca.

P: kita ada gak sih pak IP analisa tentang produk atau layanan colo ini? Kelebihannya apa, kekurangannya apa?

I: analisa SWOT? Wah kalo begitu kita belum bikin tuh, paling juga anak marketing punya tuh buat bikin strategi pemasaran mereka, tapi kalo kita bikin sendiri dari facility sih belum ada ya, ide bagus tuh sih ya., kalo anak marketing kan pasti analisanya banyak miss soal teknisnya sih ya. Kita sih sekarang itu belum ada, coba lo Tanya sama si dina soal itu

P:pak jadi selama ini belum ada nih bikin project buat analisa risiko?

I: belum pernah yang secara resmi kita terrapin satu persatu tahapannya yang kayak lo maksud, tapi kita mendekati lah ya, gak mungkin juga perusahaan kayak gini gak care sama risiko, kita bisa bertahan selama ini juga pasti karena risiko yang kita hadepin kan kecil ya, selama ini sih kita masih melakukan preventif, pencegahan aja dengan melakukan tahapan SOP dengan baik.

P: pak kalo keselamatan kerja kita punya gak?

I: apaan? Kayak K3? Wah kita belum ada tuh, HRDnya juga gak ngurus kayaknya, tapi kita kana da jamsostek, kalo dari kantor sih peralatan buat K3 ada, buat yang dilapangan tapi biasa lah orang Indonesia kalo masalah begituan masih ngerasa ribet.

LAMPIRAN 5

Wawancara dengan AG, staf keamanan data center PT "X" pada tanggal 8 maret 2012, pukul 22.00 WIB

P: Peneliti

I:Informan

P:Mas mau Tanya-tanya yah, kemarin kan saya udah kasih tau mas AG kalo bakal nanya2 buat skripsi, ahahahahaha

I:Iya gapapa mba vega Tanya aja, mau nanya apaan? Kok belum pulang udah malem begini?

P:Iya nih, tadi ujan juga diluar yaudah sekalian aja nanya-nanya dulu sama mas AG

I: Oh emang ujan ya? Yaudah sini aja dulu mbak nanya2

P:yaudah mas, mau kesitu dong (masuk keruangan sekuriti)

I:Nih mbak ID nya (Memberikan ID card akses masuk kedalam area data center)

P:Mas,ini shifnya berapa kali si? Kmrn nanya pa A katanya 2 kali ya shift ya sehari?

I:Iya mbak,sehari dua kali,2 kali duabelas jam

P:12 jam?

I:Iya jadi kerjanya 12 jam

P:lah orang kan jam kerja sehari Cuma 8 jam mas, itu 12 jam ga diitung lembur?

I:Ya nggak mbak, namanya juga sekuriti emang begitu jaganya, ahahahahah

P:Oh 12 jam nya itu gimana baginya?

I:Iya jadi dating jam 8 pagi pulang jam 8 malem kalo yg shift pagi, kalo yang shift malem ya dating dari jam 8 pulang jam 8 malem.

P: lah ini kok mas AG sendirian? Aturan tugas sama siapa atuh?

I:sama mas alan, dia lagi ke toilet kali mbak.

P: Ooo ini gimana sih cara ngebukainnya? (peneliti menanyakan bagaimana membuka pintu masuk ke lantai 6 dari meja sekuriti tanpa menggunakan ID card)

I:Ini disini ada tombolnya nih mbak, dibawah meja sini, jadi kalo orang luar yang mau masuk tapi ga punya ID card kita bukain pake ini. Tadi tuh mbak yang namanya mas alan (menunjukan sekuriti lainnya)

P: Eh mas AG, kalo ngamanin-ngamanin kayak gini ada SOPnya gak sih?

I: SOP? Maksudnya mbak? (Informan tidak mengerti apa itu SOP)

P: maksudnya harusnya ada dokumennya gitu,prosedurnya, syarat-syarat orang boleh masuk harus gimana misalnya orang dating harus isi ini dulu, harus kemana dulu gitu, peraturannya gitu loh mas, ada gak?

I:Iya adalah mbak,

P:yang ngasih dokumen kayak gitu siapa, persyaratan-persyaratannya?

I:Facility, si pak Andi, (menyebutkan nama manajer facility) jadi dia, misalnya kan customer kita PT X (menyebutkan nama perusahaan telekomunikasi asal china) kalo dulu kan kalo buat masuknya kan dia nulisnya manual tuh mbak nulis di formnya. Kalo sekarang tuh datanya diminta dulu sama Pak Andi , nanti pak Andi yang proses buat email sama log in masuk ke data centernya, kan ini ada log in elektronik nih mbak, itu tuh computer yang itu (menunjuk ke computer yang ada didepan) jadi ntar kalo dia dating dia tinggal masukin id sama password yang udah dikasi sama pak andi

P:Ohhh gitu, masnya udah berapa lama sih disini?

I:baru mbak, baru 4 bulan

P:Ohhh baru toh

I: iya mbak jadi gitu, kalo dia udah log in, ntar dia ke saya buat minta kunci, nah saya kasih deh kunci rack nya dia,paling disimpen ID sama KTPnya dia selama dia masuk didalem

P: disimpen selama dia masuk? Udah keluar baru diambil? Paling lama berapa lama tuh dia didalem mas?

I:tergantung mbak, lagian kita juga gak bisa prediksi dia dating jam berapa terus keluar jam berapa

P:kenapa emangnya? Bisa lama dia didalem?

I:waktu itu sih bisa semaleman dia sampe pagi

P:semaleman? Ngapain itu dia semaleman?

I:ya nggak tau, ngapain mbak, say amah gak ngerti. Ya mungkin ada kali tugasnya dari kantornya

P:semaleman? Itu misalnya dia servernya di data center 1, bisa gak masuk ke data center 2?

I:ya ngga bisa lah mbak, kecuali kalo emang servernya dia di 2 ya dia bisa masuk kesitu. Kalo misalnya gak ada ya ga boleh, keperluannya ngapain masuk kesitu

Tiba-tiba mas alan datang dan menanyakan kehadiran peneliti diruangan sekuriti,menanyakan kenapa peneliti hanya interview AG

P: mau nanya2 aja mas, mau interview biar si mas AG kayak artis. Hahahahah

P: mas ini catetan-catetan gini kalo ada yang dating juga dipake?

I: catetan mah ini paling disini, customer buat kita catet, iya ini juga masih dipake sih yang manual

P: terus ini catetan di laporinnya kesiapa ya? Ke facility juga?

I: kalo itu gak tau juga ya, selama saya kerja disini sih itu belom diperiksa-periksa,

P: iyah? Belum diperiksa-periksa selama 4 bulan? Mas AG disini udah 4 bulan kan berarti?

I: iya tau tuh kenapa

P: wah kok bisa belum diperiksa ya

I: palingan diperiksanya dari sini (menunjukan system intranet dikomputer) jadi kana da dua inputan mbak, manual sama yang elektronik pake log in. kalo ini catatan buat kita aja kali ya sekuriti. Paling orang dalem yngeceknya dari sini (buku manual) karena kan gak semua bisa liat akses masuknya

P: iya sih saya gak bisa, eh mas pernah gak sih ada yang datang tapi dia gak nunjukin semua persyaratannya yang lengkap tapi dikasih masuk?

I: lupa atau gimana gitu? Nggak lah gak mungkin

Soalnya kan kalo dia main masuk aja tapi gak bilang dulu sama kita (sekuriti)n dia masuk pake apa?

P:nggak, misalnya aturan dia isi dulu tapi dia gak isi main minta kunci

I: oh kita gak kasih izin mbak, kecuali dia telepon atasannya, atasannya telepon Pak Andi, terus pak andi nya ya informasiin ke sekuritibaru kita kasih

P: emang yang ditakutin apaan sih mas makanya gak boleh sembarang orang yang boleh masuk?

I: yakan itu banyak server punya orang juga kan mbak, kan namanya juga antisipasi, takutnya dia ngapa-ngapain didalem kan

P: ini CCTV aktif semua nih? (sambil menunjuk layar monitor CCTV)

I: aktif semua mbak

P: mana coba liat mana yang DC 1?

I: nih,nih (informan menunjukan monitor pemantau CCTV)

P: kenapa gelap mas?

I: bentar-bentar

P: oh gitu

I: ini DC 3 nih secure cage yang dikarengkeng, ini DC 1 nih yang pas pintu keluar nih,ini ruang metro nih yang kedua DC 2,

P: ini direkam apa Cuma diliat doing?

I: direkam mbak, tapi yang punya rekamannya yang punya mas sigit deh kalo gak salah

P: kalo misalnya yang dulu gak ada gak dokumen yang sebelumnya ada terus harus diterusin sama mas AG? Kalo kayak gini kan emang udah ada.

I: hmmm, ada nya kayak gini sih mbak, daftar kunci. Kan kalo pelanggan kuncinya ada nomer racknya, kita mana afal semuanyanha ya ini ada daftarnya sama lokasi servernya dimana, sama ini lagi ada daftar siapa aja yang ngeganti password yang udah dikasih sama pak Andi

P: emang kalo mereka ganti password kit bisa tau?

I: ya kan pas dikasih pertama kali itu bisa diganti bisa juiga nggak

P: ohh kayak gini ya bagannya, DC 1 30 DC2 52 yah, itu kalo kunci-kuncinya itu masnya tau tuh letak-letaknya dimana aja, apa itu daftar juga dapet dari facility juga?

I: kalo ini kita dikasih tau sama facility sih mbak, itu kan tadi udah ada daftarnya tuh, kunci nomer berapa rack nomer berapa

P: oh jadi gitu ya, dating, isi lag in, minta kunci, mas kasih kunci sama ID card baru dia masuk ya

I: iya, kayak gini loh mbak, (memperlihatkan tempat kunci) kalo yang ini kunci pelanggan semua nih mbak, kalo yang ini kunci mobil, kalo yang ini kunci motor punya anak HFC (etugas penarikan kabel untuk internet)

P: hooo, itu kunci-kunci yang lain mintanya kesini juga? Harus inget juga dong semuanya?

I: kan ini mbak ada catetannya (menunjukan catetan daftar kunci yang lain)

P: berarti yang dijagain bukan data center aja

I: iya sih mbak, tugasnya gak terlalu ke sekuriti kalo saya rasa mah lebih berat ke admin, hahahaha. Oiya motor juga kesini ambil kuncinya. Kalo mau booking pake mobil juga kesini mbak telfonnya, nyari orang telfonnya juga kesini, ntar kuncinya dibalikin juga kesini lagi mbak kuncinya

P: wah kayak operator aja dong sampe segala terima telfon masuk juga

I: Iya mbak, ahahahhahahha jadi kita gak Cuma sekuriti aja sih mbak, kerjanya lebih ke admin

I: kalo tampilan di log in dikomputernya kayak gini nih mbak (memperlihatkan log in elektronik di intranet) kalo kuning berate kan udah pulang nih, kalo putin masih didlem orangnya, nah kalo merah di cancel kunjungan ke data centernya mbak

P: Ohh gitu, kalo saya bisa request juga gak?

I: bisa juga mbak, tuh pilih engineering, pilih data center, pilih request form (menunjukan menu di intranet)

P: hoo, ini resuest dari orang dalem ya, si mas andri masuk bawa customer nya dia ya? kalo yang dari luar bisa keliatan juga nggak?

I:iya itu si mas andri bawa kustomernya dia kalo yang dari luar mbak?ohh bisa, nih kalo itu tadi kan request internal, nah kalo ini nih yang daftar customer yang dating

P:oooh jadi yang punya akses ini Cuma facility sama security ya,

I: iya kalo security bisa liat buat control gitu, oiya nih belum ditutup (AG lupa menutup akses masuk customer yang sudah selesai kunjungan sehingga di tabel masih berwarna putih padahal customer sudah keluar sejak lama)

P:ini yang merah dicancel nih?

I: cancel

P: gak jadi dateng?

I: iya

P: loh sebelumnya dia bilang mau dating emang via apa? Telfon?

I: nggak mbak, kan suka tuh abis dia log in minta ID segala macem ada yang mau langsung masuk ada yang dia makan dulu lah, eh ga jadi dateng dia telfon kesini, nah kita tutup pake warna merah, artinya dia cancel.

P: hooo, jadi yang namanya keburu masuk tapi gak jadi dating

I:iya nanti kita cancel

P: paling lama berapa lama itu mas pelanggan kalo masuk ke data center

I: ada yang sampe semaleman mbak

P: hah yang bener aja, masa semaleman mas di ruang server, secara itu kan digin banget plusminus 16

I: ya kan dia pake jaket mbak, pernah itu malem masuknya

P: paling malem dating jam berapa itu orangnya?

I: jam 4 pagi baru dating juga pernah mbak

P: jam 4 pagi? Setan kali itu mas? Hahahahhahah

I: iya, sampe setengah tujuh baru keluar dating dari jam 9 malem juga pernah mbak

P: ah sinting-sinting banghet itu orang, pasti aneh deh begadang diruang server.

I: pernah juga yang keluar dulu, makan pop mi dulu, ntar masuk lagi juga ada mbak, yah lagi banyak kali mbak kerjaannya, pokoknya kalo dateng malem-malem udah pake jacket bawa bekel segala pasti mau nginep lah disini itu mah

P: Oh gitu, jadi dia kalo udah masuk, terus keluar kalo mau masuk harus isi log in lagi?

I: nggak usah mbak, ntar kan yang nutup aksesnya kita

P:kalo udah selesai?

I:pokoknya mah kalo dia udah selesai kan otomatis dia ngasih kunci balik nih, nah disitu kita kan tau dia udah selesai, baru kita tutup aksesnya mbak

P:pernah lupa nggak?

I: pernah,yang penting dari kitanya gak boleh teledor, siapa nih yang terakhir pake, misalnya bapak dibyo dari pt x (menyebutkan nama maskapai perebangan) langsung telfon minta maaf lah

P: ohh kebawa gitu kuncinya?

I: iya mbak, kunci mobil juga pernah tuh, mbak tau mbak else kan? Waktu itu dia marah-marah gara-gara saya lupa kasih kunci, padahal mah seinget saya dia gak pernah request

P:yaelah mas, si else mah gak usah didenger emang orangnya kayak gitu

I:oh emang orangnya kayak gitu ya mbak? Iya sih tapi kan namanya saya bawahan mbak pasti salah saya lah

P: udah mas dia mah diemin aja, ini warna putih orangnya masih ada didalem nih?

I: nggak mbak itu juga lupa di close

P: ooh, ini kayak gini reportnya per berapa bulan mas?

I: kayaknya sih perbulan deh mbak, soalnya kan kayak report mobil juga perbulan kan

P: oh gitu,ini kalo dateng dia perlu bilang gak sih keperluannya buat apa?

I: ditaro di note sih mbak itu,

P: ooh ini ya keperluannya, pasang kabel UTP,tapi ini sebenernya harus diissi gak sih keperluannya ngapain

I: nggak sih, kita kan gak perlu tau juga dia ngapain, asal dia ngutak-atik servernya sendiri mah itu urusannya dial ah mbak kita gak perlu tau. Yang pasti kalo ada sesuatu yang ganjil kita kan tau yang terakhir masuk siapa

P: paling aneh ngapain ya?

I: paling aneh? Customer maksudnya?

P: iya paling anhe customer dateng tuh buat apa?

I: ya gak tau juga mbak, kita kan gak mantengin juga selama dia dateng ngapain aja

P: ooo jadi yang paling aneh ya itu ya mas, dateng jam stengah 4 pagi sama makan popmi, ahahahahhaha

I:iya mbak itu aneh banget, saya aja lucu ingetnya, ada juga mbak yang lucu, dateng ngobrol-ngobrol dulu, dateng Cuma 15 menit terus keluar lagi, saya juga gak negrti ngapain itu masuk Cuma 15 menit sebentar banget, hhahaha kocak deh mbak,itu yang suka kayak gitu si pak gunawan dari pt x (menyebutkan nama perusahaan mining) dia baik sih orangnya.

P: ngapain atuh 15 menit doing, ngadem kali mas, naik motor. ngecek doing kali ya

I: udah gitu kan sekuriti kan kayak customer service juga, bikin report ada siapa aja yang dateng, dari branch juga lapornya kesini mbak

P: jadi gak focus ya,

I: ya gitu sih mbak,

P: ini ambil barang barang apa ya maksudnya? (menanyakan keterangan di log in masuk) tau gak?

I: ambil barang dia, server dia di ambil lagi, ntah diambil ntah diganti.

P: hooo,banyak juga ya, trouble shooting, maintenance,cek server, repsrt katru 3, ganti kartu (menyebuykan nama provider) cabling,

I: dari sini kan bisa keliatan nih mbak siapa aja yang rajin dateng,

P: tiap hari dia dateng? Ada gak sih mas yang jarang dateng? Itu seharusnya dia dateng seminggu sekali atau gimana sih?

I: itu sih tergantung dari perusahaannya mbak, kalo kayak si x (menyebutkan nama perusahaan start up) udah lama ga dateng, harang dateng di amah

P: kelo selain itu rutin?

I:selain itu ya lumayan rutin sih

P: ini kalo keterangan yang nulis dia sendiri kan?

I: iya dia sendiri mbak pas log in

P: tapi kalo gak disi juga gak apa-apa?

I: gak apa-apa

P:, ooo jadi isinya ticket id, customer id, nama perusahaan, yang dateng siapa,id card nya berapa, id card number yang mana mas?

I: yang ini mbak, yang kita kasih buat dia masuk

P: aktifitasnya ngapain, jam masuknya,jam keluarnya, statusnya, apr maksudnya apaan mas?

I: apr di approve

P: ada yang di reject gak?

I: di reject ya di cancel tadi mbak

Mas AG terima telfon dari branch

P: tapi kalo pake data-data kayak gini tuh ngebantu kerjaan?

I: iya lah mbak,kalo ada ini kan bisa nyontek nih, tapi rata-rata customer baik-baik sih mbak, suka ngrobrol gitu.

P: ini nomer kunci sampe seratus nih mas? Kan tadi customernya cuma ada 82?

I: iya mbak, tapi kan 1 perusahaan ada yang nyewa 2, ya jadi nomer kuncinya bisa dobel-dobel.

P: Hoooo gitu mas, eh mas AG udah male mini, saya pulang dulu deh ya, ntar kalo ada yang ga jelas saya nanya-nanya lagi loh yaaa

I; sok atuh mbak vega nanya-nanya aja gapapa say amah.

P: yaudah nuhun loh mas AG, saya masuk dulu ya siap-siap pulang

Wawancara dengan Y.U sales data center pada tanggal 24 Maret 2012 pukul 08.30 WIB

P: Peneliti

I: Informan

P: pagi mbak, nanya-nanya dong soal data center

I: boleh veg,sini nanya aja

P: mbak ada kita punya gak sih dokumen standarisasi kualitas layanan yang kita kasih?

I: hmm, kalo itu belum dirumusin sih ya, kita masih mengacu sama SLA, Service Level Agreement, didalemnya kana da spesifikasi alat yang kita pake apa aja dan apa aja yang harus kita lakuin, kayak pemantauan suhu berapa kali, dan lain-lain, SLA untuk data center itu 99,99% jadi emang gak boleh ada down timenya namanya juga data center ya, dia kan naro aplikasi juga disitu kalo mati bisa rugi milyaran itu customer

P: itu 99,99 % yang 1 %nya lagi itu force majeur ya berarti? Nah 1 % nya itu berapa lama mbak dalam setahun? Kalo lebih dari itu gimana?

I: iya itu dalem setahun, wah itu sih kalo aku gak salah dalam hitungan detik ya 1 %ny itu, kalo masalah ganti rugi nya sih belum dibakukan secara eksaknya berapa soalnya kan banyak aspek yang harus dilihat juga yang jelas gak boleh mati, that's why kita ada redundant nya

P: kalo analisa SWOT tim sales punya ya mbak? Tapi itu lebih ke komunikasinya? Teknis nya ada juga gak?

I: analisa SWOT iya sih, kita punya kalo dari tim sales marketing itu lebih ke SWOT buat jualan ya, kayak gimana competitor beriklan, strateginya mereka kayak gitu

lah, bukan SWOT yang teknis bangetPI: nah kalo faktor-faktor yang mempengaruhi data center bikin juga gak?

I: wah itu sih belum pernah bikin ya, soalnya kan udah hamper sama juga apa-apa aja yang jadi faktor sama apa yang ada di SWOT tapi seharusnya kalo terkait sama risiko mah soal faktor-faktor begitu aturan tanya si AS bukan? Kan dia tuh yang ngurusin SOP buat standarisasi aturan dy punya ya, jangan tanya sales"

P: Kalo product analysis bikin nggak mbak?

I: ada sih kalo product analysis, itu yang bikin product manajernya, isinya tentang product knowledge, janji yang dikasih ke para calon customer apa, dan gimana cara mendeliver janji tersebut dengan baik, semua ntar yg handle si product manajer, tapi posisi itu kan baru, nanti tiap product punya PM sendiri